ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/260712666

Internet of Things Strategic Research and Innovation Agenda

Chapter · January 2013

CITATIONS
88

READS
4,849

8 authors, including:

Patrick Guillemin
European Telecommunications Standards Institute
24 PUBLICATIONS **1,742** CITATIONS
SEE PROFILE

Harald Sundmaeker
Institut für angewandte Systemtechnik Bremen GmbH
47 PUBLICATIONS **1,978** CITATIONS
SEE PROFILE

Markus Eisenhauer
Luxembourg Institute of Science and Technology (LIST)
48 PUBLICATIONS **1,368** CITATIONS
SEE PROFILE

Klaus Moessner
University of Surrey
335 PUBLICATIONS **4,813** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

H2020 CLEAR 5G View project

BEMO-COFRA - Brazil-Europe – Monitoring and Control Frameworks View project

All content following this page was uploaded by Patrick Guillemin on 21 May 2014.

The user has requested enhancement of the downloaded file.

River Publishers Series in Communications

Internet of Things — Converging Technologies for Smart Environments and Integrated Ecosystems

Editors
Ovidiu Vermesan
Peter Friess

River Publishers

Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems

RIVER PUBLISHERS SERIES IN COMMUNICATIONS

Consulting Series Editors

MARINA RUGGIERI
University of Roma "Tor Vergata"
Italy

HOMAYOUN NIKOOKAR
Delft University of Technology
The Netherlands

This series focuses on communications science and technology. This includes the theory and use of systems involving all terminals, computers, and information processors; wired and wireless networks; and network layouts, procontentsols, architectures, and implementations.

Furthermore, developments toward new market demands in systems, products, and technologies such as personal communications services, multimedia systems, enterprise networks, and optical communications systems.

- Wireless Communications
- Networks
- Security
- Antennas & Propagation
- Microwaves
- Software Defined Radio

For a list of other books in this series, please visit www.riverpublishers.com.

Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems

Dr. Ovidiu Vermesan
SINTEF, Norway

Dr. Peter Friess
EU, Belgium

River Publishers

Aalborg

Published, sold and distributed by:
River Publishers
PO box 1657
Algade 42
9000 Aalborg
Denmark
Tel.: +4536953197

www.riverpublishers.com

ISBN: 978-87-92982-73-5 (Print)
ISBN: 978-87-92982-96-4 (E-Book)
© 2013 River Publishers

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Dedication

"A rock pile ceases to be a rock pile the moment a single man contemplates it, bearing within him the image of a cathedral."

— Antoine de Saint-Exupéry

"Creativity is contagious. Pass it on."

— Albert Einstein

Acknowledgement

The editors would like to thank the European Commission for their support in the planning and preparation of this book. The recommendations and opinions expressed in the book are those of the editors and contributors, and do not necessarily represent those of the European Commission.

Ovidiu Vermesan
Peter Friess

This page intentionally left blank

Editors Biography

Dr. Ovidiu Vermesan holds a Ph.D. degree in microelectronics and a Master of International Business (MIB) degree. He is Chief Scientist at SINTEF Information and Communication Technology, Oslo, Norway. His research interests are in the area of microelectronics/nanoelectronics, analog and mixed-signal ASIC Design (CMOS/BiCMOS/SOI) with applications in measurement, instrumentation, high-temperature applications, medical electronics and integrated sensors; low power/low voltage ASIC design; and computer-based electronic analysis and simulation. Dr. Vermesan received SINTEFs 2003 award for research excellence for his work on the implementation of a biometric sensor system. He is currently working with projects addressing nanoelectronics integrated systems, communication and embedded systems, integrated sensors, wireless identifiable systems and RFID for future Internet of Things architectures with applications in green automotive, internet of energy, healthcare, oil and gas and energy efficiency in buildings. He has authored or co-authored over 75 technical articles and conference papers. He is actively involved in the activities of the European Technology Platforms ENIAC (***E**uropean **N**anoelectronics **I**nitiative **A**dvisory **C**ouncil*), ARTEMIS (***A**dvanced **R**esearch & **T**echnology for **EM**bedded **I**ntelligence and **S**ystems*), EPoSS (***E**uropean Technology **P**latform **o**n **S**mart **S**ystems Integration*). He coordinated and managed various national and international/EU projects related to integrated electronics. He was co-coordinator of ENIAC E^3Car project, and is currently coordinating the ARTEMIS projects POLLUX and IoE — Internet of Energy for Electric Mobility. Dr. Vermesan is the coordinator of the IoT European Research Cluster (IERC) of the European Commission, actively participated in EU FP7 Projects related to Internet of Things.

Dr. Peter Friess is a senior official of the European Commission overseeing for more than five years the research and innovation policy for the Internet of Things, Machine to Machine communication and related subject areas such as Smart Cities, Cloud computing, Future Internet, Trust and Security. In this function he has shaped the on-going European research and innovation program on the Internet of Things and became responsible for supervising the European Commission's direct investment for 70 Mill. Euro in this field. As part of the Commission Internet of Things European

Action Plan from 2009, he also oversees international cooperation on the Internet of Things, in particular with Asian countries.

In previous engagements he was working as senior consultant for IBM, dealing with major automotive and utility companies in Germany and Europe. Prior to this engagement he worked as IT manager at Philips Semiconductors dealing with business process optimisation in complex manufacturing. Before that period he was active as a researcher in European and national research projects on advanced telecommunications and business process reorganisation.

He is a graduate engineer in Aeronautics and Space technology from the University of Munich and holds a Ph.D. in Systems Engineering including self-organising systems from the University of Bremen. He also published a number of articles and co-edits a yearly book of the European Internet of Things Research Cluster.

Foreword

The Bright Future of the Internet of Things

Mário Campolargo
DG CONNECT, European Commission, Belgium

"*IoT will boost the economy while improving our citizens' lives*"

Analysts predict that new Internet of Things (IoT) products and services will grow exponentially in next years. I firmly believe that the Commission will continue to support research in IoT in Horizon 2020, the forthcoming EU research and innovation framework programme starting in 2014.

In order to enable a fast uptake of the IoT, key issues like identification, privacy and security and semantic interoperability have to be tackled. The interplay with cloud technologies, big data and future networks like 5G have also to be taken into account.

Open and integrated IoT environments will boost the competitiveness of European SMEs and make people's daily life easier. For instance, it will be easier for patients to receive continuous care and for companies to efficiently source components for their products. This will lead to better services, huge savings and a smarter use of resources.

To achieve these promising results, I think it is vital to enhance users' trust in the Internet of Things. The data protection legislation and the cybersecurity strategy proposed by the European Commission clearly go in this direction.

I am confident that the following chapters will cater for interesting reading on the state-of-the-art of research and innovation in IoT and will expose you to the progress towards the bright future of the Internet of Things.

Contents

Foreword
The Bright Future of the Internet of Things **ix**
Mário Campolargo

1 Driving European Internet of Things Research **1**
Peter Friess

1.1 The Internet of Things Today 1
1.2 Time for Convergence 3
1.3 Towards the IoT Universe(s) 5
1.4 Conclusions 6

2 Internet of Things Strategic Research and Innovation Agenda **7**
Ovidiu Vermesan, Peter Friess, Patrick Guillemin, Harald Sundmaeker, Markus Eisenhauer, Klaus Moessner, Franck Le Gall, and Philippe Cousin

2.1 Internet of Things Vision 7
2.2 IoT Strategic Research and Innovation Directions 16
2.3 IoT Applications 39
2.4 Internet of Things and Related Future Internet Technologies 61
2.5 Infrastructure 69
2.6 Networks and Communication 72
2.7 Processes 78
2.8 Data Management 81
2.9 Security, Privacy & Trust 92
2.10 Device Level Energy Issues 95

2.11 IoT Related Standardization 101
2.12 Recommendations on Research Topics 113
References 144

3 IoT Applications — Value Creation for Industry 153

Nicolaie L. Fantana, Till Riedel, Jochen Schlick, Stefan Ferber, Jürgen Hupp, Stephen Miles, Florian Michahelles, and Stefan Svensson

3.1 Introduction 154
3.2 IoT Applications for Industry — Value Creation and Challenges 155
3.3 Future Factory Concepts 162
3.4 Brownfield IoT: Technologies for Retrofitting 171
3.5 Smart Objects, Smart Applications 177
3.6 Four Aspects in your Business to Master IoT 180
3.7 Auto_ID — Value Creation from Big Data and Serialization in the Pharmaceutical Industry 186
3.8 What the Shopping Basket Can Tell: IoT for Retailing Industry? 194
3.9 IoT For Oil and Gas Industry 197
3.10 Opinions on IoT Application and Value for Industry 201
3.11 Conclusions 204
References 204

4 Internet of Things Privacy, Security and Governance 207

Gianmarco Baldini, Trevor Peirce, Marcus Handte, Domenico Rotondi, Sergio Gusmeroli, Salvatore Piccione, Bertrand Copigneaux, Franck Le Gall, Foued Melakessou, Philippe Smadja, Alexandru Serbanati, and Julinda Stefa

4.1 Introduction 207
4.2 Overview of Activity Chain 05 — Governance, Privacy and Security Issues 211
4.3 Contribution From FP7 Projects 212
4.4 Conclusions 223
References 224

5 Security and Privacy Challenge in Data Aggregation for the IoT in Smart Cities **225**
Jens-Matthias Bohli, Peter Langendörfer, and Antonio F. Gómez Skarmeta

5.1 Security, Privacy and Trust in Iot-Data-Platforms for Smart Cities 226
5.2 First Steps Towards a Secure Platform 228
5.3 Smartie Approach 236
5.4 Conclusion 240
References 241

6 A Common Architectural Approach for IoT Empowerment **245**
Alessandro Bassi, Raffaele Giaffreda, and Panagiotis Vlacheas

6.1 Introduction 245
6.2 Defining a Common Architectural Ground 247
6.3 The iCore Functional Architecture 251
References 257

7 Internet of Things Standardisation — Status, Requirements, Initiatives and Organisations **259**
Patrick Guillemin, Friedbert Berens, Marco Carugi, Marilyn Arndt, Latif Ladid, George Percivall, Bart De Lathouwer, Steve Liang, Arne Bröring, and Pascal Thubert

7.1 Introduction 259
7.2 M2M Service Layer Standardisation 262
7.3 OGC Sensor Web for IoT 266
7.4 IEEE and IETF 270
7.5 ITU-T 272
7.6 Conclusions 275
References 276

8 Simpler IoT Word(s) of Tomorrow, More Interoperability Challenges to Cope Today **277**
Payam Barnaghi, Philippe Cousin, Pedro Maló, Martin Serrano, and Cesar Viho

8.1 Introduction 277
8.2 Physical vs Virtual 283
8.3 Solve the Basic First — The Physical Word 285
8.4 The Data Interoperability 290
8.5 The Semantic Interoperability 293
8.6 The Organizational Interoperability 299
8.7 The Eternal Interoperability [28] 299
8.8 The Importance of Standardisation — The Beginning of Everything 303
8.9 The Need of Methods and Tools and Corresponding Research 304
8.10 The Important Economic Dimension 307
8.11 The Research Roadmap for IoT Testing Methodologies 308
8.12 Conclusions 309
References 312

9 Semantic as an Interoperability Enabler in Internet of Things 315
Vicente Hernández Díaz, José Fernán Martínez Ortega, Alexandra Cuerva García, Jesús Rodríguez-Molina, Gregorio Rubio Cifuentes, and Antonio Jara

9.1 Introduction 315
9.2 Semantics as an Interoperability Enabler 322
9.3 Related Works 335
9.4 Conclusions 339
References 340

Index 343

1

Driving European Internet of Things Research

Peter Friess

European Commission, Belgium

1.1 The Internet of Things Today

One year after the past edition of the Clusterbook 2012 it can be clearly stated that the Internet of Things (IoT) has reached many different players and gained further recognition. Out of the potential Internet of Things application areas, Smart Cities (and regions), Smart Car and mobility, Smart Home and assisted living, Smart Industries, Public safety, Energy & environmental protection, Agriculture and Tourism as part of a future IoT Ecosystem (Figure 1.1) have acquired high attention.

In line with this development, the majority of the governments in Europe, in Asia, and in the Americas consider now the Internet of Things as an area of innovation and growth. Although larger players in some application areas still do not recognise the potential, many of them pay high attention or even accelerate the pace by coining new terms for the IoT and adding additional components to it. Moreover, end-users in the private and business domain have nowadays acquired a significant competence in dealing with smart devices and networked applications.

As the Internet of Things continues to develop, further potential is estimated by a combination with related technology approaches and concepts such as Cloud computing, Future Internet, Big Data, robotics and Semantic

Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, 1–6.
© 2013 *River Publishers. All rights reserved.*

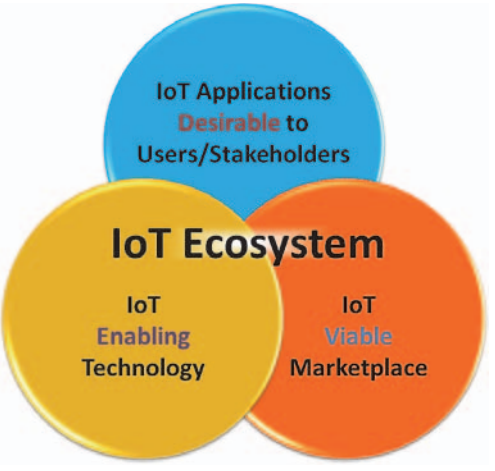

Fig. 1.1 IoT Ecosystem.

technologies. The idea is of course not new as such but becomes now evident as those related concepts have started to reveal synergies by combining them.

However, the Internet of Things is still maturing, in particular due to a number of factors, which limit the full exploitation of the IoT. Among those factors the following appear to be most relevant:

- No clear approach for the utilisation of unique identifiers and numbering spaces for various kinds of persistent and volatile objects at a global scale.
- No accelerated use and further development of IoT reference architectures like for example the Architecture Reference Model (ARM) of the project IoT-A.
- Less rapid advance in semantic interoperability for exchanging sensor information in heterogeneous environments.
- Difficulties in developing a clear approach for enabling innovation, trust and ownership of data in the IoT while at the same time respecting security and privacy in a complex environment.
- Difficulties in developing business which embraces the full potential of the Internet of Things.
- Missing large-scale testing and learning environments, which both facilitate the experimentation with complex sensor networks and stimulate innovation through reflection and experience.

- Only partly deployed rich interfaces in light of a growing amount of data and the need for context-integrated presentation.
- Practical aspects like substantial roaming-charges for geographically large-range sensor applications and missing technical availability of instant and reliable network connectivity.

Overcoming those hurdles would result in a better exploitation of the Internet of Things potential by a stronger cross-domain interactivity, increased real-world awareness and utilisation of an infinite problem-solving space. Here the subsequent chapters of this book will present further approaches and solutions to those questions.

In addition eight new projects from the recent call on SMARTCITIES in the scope of the European Research Program FP7, including a support and coordination action on technology road-mapping, will reinforce this year the research and innovation on a safe/reliable and smart Internet of Things, and complete the direct IoT related funding of 70 M€ in FP7. Furthermore, a project resulting from a joint call with Japan will explore the potential of combining IoT and Cloud technologies.

1.2 Time for Convergence

Integrated environments that have been at the origin of the successful take up of smartphone platforms and capable of running a multiplicity of user-driven applications and connecting various sensors and objects are missing today. Such super-stack like environments, bringing together a number of distinct constituencies, represent an opportunity for Europe to develop Internet of Things ecosystems. As an example this would include the definition of open APIs and hence offer a variety of channels for the delivery of new applications and services. Such open APIs are of particular importance at module range on any abstraction level for application-specific data analysis and processing, thus allowing application developers to leverage the underlying communication infrastructure and use and combine information generated by various devices to produce added value across multiple environments.

As a quintessence the next big leap in the Internet of Things evolution will be the coherence of efforts on all levels towards innovation (Figure 1.2). In case of the IoT community this would mean that out of many possible “coherence

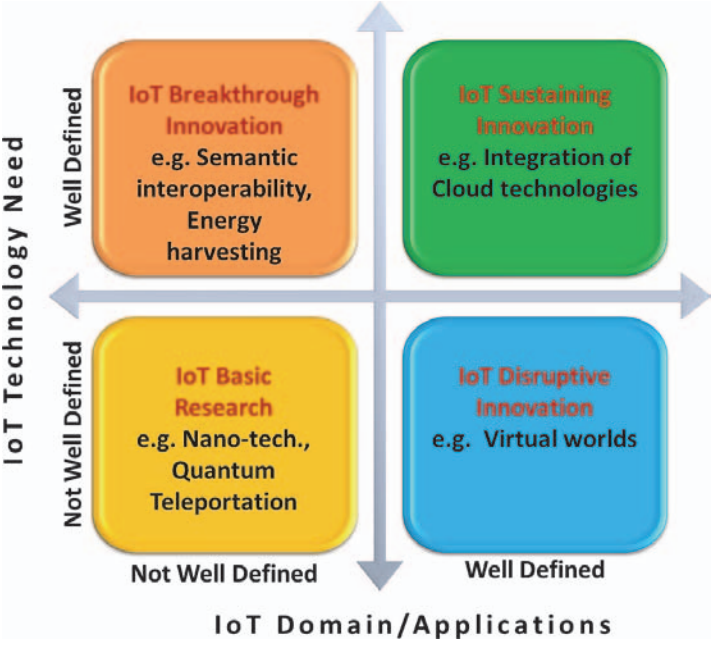

Fig. 1.2 Innovation Matrix of IERC — Internet of Things European Research Cluster.

horizons" the following will likely provide the foundation for a step forward to the Internet of Things:

- *Coherence of object capabilities and behaviour*: the objects in the Internet of Things will show a huge variety in sensing and actuation capabilities, in information processing functionality and their time of existence. In either case it will be necessary to generally apprehend object as entities with a growing "intelligence" and patterns of autonomous behaviour.
- *Coherence of application interactivity*: the applications will increase in complexity and modularisation, and boundaries between applications and services will be blurred to a high degree. Fixed programmed suites will evolve into dynamic and learning application packages. Besides technical, semantic interoperability will become the key for context aware information exchange and processing.

- *Coherence of corresponding technology approaches*: larger concepts like Smart Cities, Cloud computing, Future Internet, robotics and others will evolve in their own way, but because of complementarity also partly merge with the Internet of Things. Here a creative view on potential synergies can help to develop new ecosystems.
- *Coherence of real and virtual worlds*: today real and virtual worlds are perceived as two antagonistic conceptions. At the same time virtual worlds grow exponentially with the amount of stored data and ever increasing network and information processing capabilities. Understanding both paradigms as complementary and part of human evolution could lead to new synergies and exploration of living worlds.

1.3 Towards the IoT Universe(s)

In analogy to the definition that a universe is commonly defined as the totality of existence, an Internet of Things universe might potentially connect everything. As a further analogy to new theories about parallel universes, different Internet of Things worlds might develop and exist in parallel, potentially overlap and possess spontaneous or fixed transfer gates.

These forward-looking considerations do certainly convey a slight touch of science fiction, but are thought to stimulate the exploration of future living worlds. The overall scope is to create and foster ecosystems of platforms for connected smart objects, integrating the future generation of devices, network technologies, software technologies, interfaces and other evolving ICT innovations, both for the society and for people to become pervasive at home, at work and while on the move. These environments will embed effective and efficient security and privacy mechanisms into devices, architectures, platforms, and protocols, including characteristics such as openness, dynamic expandability, interoperability of objects, distributed intelligence, and cost and energy-efficiency.

Whereas the forthcoming Internet of Things related research in the scope of Horizon 2020 and corresponding national research programs will address the above matters, challenges from a societal and policy perspective remain

equally important, in particular the following:

- Fostering of a consistent, interoperable and accessible Internet of Things across sectors, including standardisation.
- Directing effort and attention to important societal application areas such as health and environment, including focus on low energy consumption.
- Offering orientation on security, privacy, trust and ethical aspects in the scope of current legislation and development of robust and future-proof general data protection rules.
- Providing resources like spectrum allowing pan-European service provision and removal of barriers such as roaming.
- Maintaining the Internet of Things as an important subject for international cooperation both for sharing best practises and developing coherent strategies.

1.4 Conclusions

The Internet of Things continues to affirm its important position in the context of Information and Communication Technologies and the development of society. Whereas concepts and basic foundations have been elaborated and reached maturity, further efforts are necessary for unleashing the full potential and federating systems and actors.[1]

[1] This article expresses the personal views of the author and in no way constitutes a formal or official position of the European Commission.

2

Internet of Things Strategic Research and Innovation Agenda

Ovidiu Vermesan[1], Peter Friess[2], Patrick Guillemin[3], Harald Sundmaeker[4], Markus Eisenhauer[5], Klaus Moessner[6], Franck Le Gall[7], and Philippe Cousin[8]

[1]*SINTEF, Norway*
[2]*European Commission, Belgium*
[3]*ETSI, France*
[4]*ATB GmbH, Germany*
[5]*Fraunhofer FIT, Germany*
[6]*University of Surrey, UK*
[7]*inno TSD, France*
[8]*Easy Global Market, France*

> "*Creativity is thinking up new things. Innovation is doing new things.*"
>
> ***Theodore Levitt***

> "*Innovation accelerates and compounds. Each point in front of you is bigger than anything that ever happened.*"
>
> ***Marc Andreessen***

2.1 Internet of Things Vision

Internet of Things (IoT) is a concept and a paradigm that considers pervasive presence in the environment of a variety of things/objects that through

Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, 7–151.
© 2013 *River Publishers. All rights reserved.*

wireless and wired connections and unique addressing schemes are able to interact with each other and cooperate with other things/objects to create new applications/services and reach common goals. In this context the research and development challenges to create a smart world are enormous. A world where the real, digital and the virtual are converging to create smart environments that make energy, transport, cities and many other areas more intelligent.

The goal of the Internet of Things is to enable things to be connected anytime, anyplace, with anything and anyone ideally using any path/network and any service.

Internet of Things is a new revolution of the Internet. Objects make themselves recognizable and they obtain intelligence by making or enabling context related decisions thanks to the fact that they can communicate information about themselves. They can access information that has been aggregated by other things, or they can be components of complex services. This transformation is concomitant with the emergence of cloud computing capabilities and the transition of the Internet towards IPv6 with an almost unlimited addressing capacity.

New types of applications can involve the electric vehicle and the smart house, in which appliances and services that provide notifications, security, energy-saving, automation, telecommunication, computers and entertainment are integrated into a single ecosystem with a shared user interface. Obviously, not everything will be in place straight away. Developing the technology in Europe right now — demonstrating, testing and deploying products — it will be much nearer to implementing smart environments by 2020. In the future computation, storage and communication services will be highly pervasive and distributed: people, smart objects, machines, platforms and the surrounding space (e.g., with wireless/wired sensors, M2M devices, RFID tags, etc.) will create a highly decentralized common pool of resources (up to the very edge of the "network") interconnected by a dynamic network of networks. The "communication language" will be based on interoperable protocols, operating in heterogeneous environments and platforms. IoT in this context is a generic term and all objects can play an active role thanks to their connection to the Internet by creating smart environments, where the role of the Internet has changed. This powerful communication tool is providing access to information, media and services, through wired and wireless broadband connections. The Internet of Things makes use of synergies that are generated

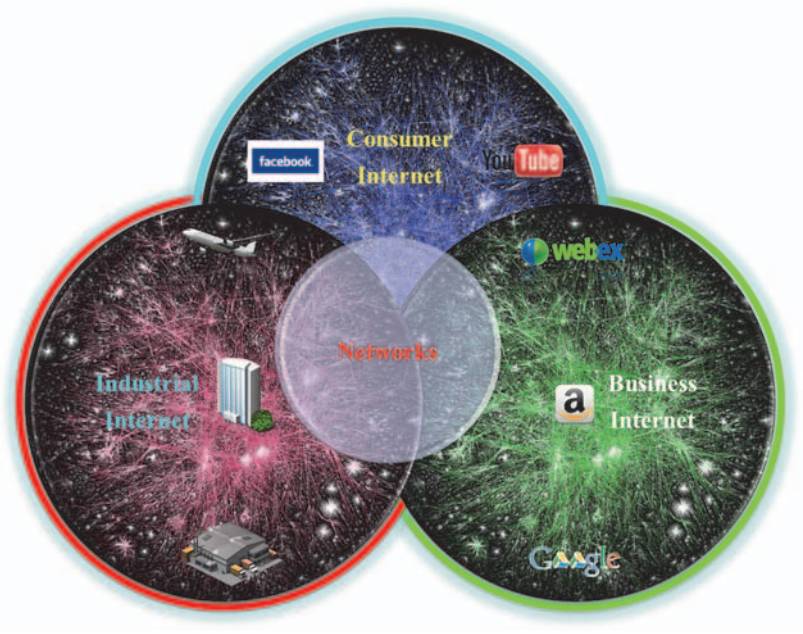

Fig. 2.1 Convergence of consumer, business and industrial internet.

by the convergence of Consumer, Business and Industrial Internet, as shown in Figure 2.1. The convergence creates the open, global network connecting people, data, and things. This convergence leverages the cloud to connect intelligent things that sense and transmit a broad array of data, helping creating services that would not be obvious without this level of connectivity and analytical intelligence. The use of platforms is being driven by transformative technologies such as cloud, things, and mobile. The cloud enables a global infrastructure to generate new services, allowing anyone to create content and applications for global users. Networks of things connect things globally and maintain their identity online. Mobile allows connection to this global infrastructure anytime, anywhere. The result is a globally accessible network of things, users, and consumers, who are available to create businesses, contribute content, generate and purchase new services.

Platforms also rely on the power of network effects, as they allow more things, they become more valuable to the other things and to users that make use of the services generated. The success of a platform strategy for IoT

can be determined by connection, attractiveness and knowledge/information/data flow.

The European Commission while recognizing the potential of Converging Sciences and Technologies to advance the Lisbon Agenda, proposes a bottom-up approach to prioritize the setting of a particular goal for convergence of science and technology research; meet challenges and opportunities for research and governance and allow for integration of technological potential as well as recognition of limits, European needs, economic opportunities, and scientific interests.

Enabling technologies for the Internet of Things such as sensor networks, RFID, M2M, mobile Internet, semantic data integration, semantic search, IPv6, etc. are considered in [1] and can be grouped into three categories: (i) technologies that enable "things" to acquire contextual information, (ii) technologies that enable "things" to process contextual information, and (iii) technologies to improve security and privacy. The first two categories can be jointly understood as functional building blocks required building "intelligence" into "things", which are indeed the features that differentiate the IoT from the usual Internet. The third category is not a *functional* but rather a *de facto* requirement, without which the penetration of the IoT would be severely reduced. Internet of Things developments implies that the environments, cities, buildings, vehicles, clothing, portable devices and other objects have more and more information associated with them and/or the ability to sense, communicate, network and produce new information. In addition we can also include non-sensing things (i.e. things that may have functionality, but do not provide information or data). All the computers connected to the Internet can talk to each other and with the connection of mobile phones it has now become mobile [2]. The Internet evolution based on the level of information and social connectivity is presented in Figure 2.2.

With the Internet of Things the communication is extended via Internet to all the things that surround us. The Internet of Things is much more than M2M communication, wireless sensor networks, 2G/3G/4G, RFID, etc. These are considered as being the enabling technologies that make "Internet of Things" applications possible.

An illustration of the wireless and wired technologies convergence is presented in Figure 2.3. In this context network neutrality is an essential element

where no bit of information should be prioritized over another so the principle of connecting anything from/to anybody located anywhere at any-time using the most appropriate physical path from any-path available between the sender and the recipient is applied in practice. For respecting these principles, Internet service providers and governments need to treat all data on the Internet equally, not discriminating or charging differentially by user, content, site, platform, application, type of attached equipment, and modes of communication.

2.1.1 Internet of Things Common Definition

Ten "critical" trends and technologies impacting IT for the next five years were laid out by Gartner in 2012 and among them the Internet of Things, which will benefit from cheap, small devices allowing that everything will have a radio and location capability. Self-assembling mesh networks, location aware services will be provided. This all creates the always on society.

In this context the notion of network convergence using IP as presented in Figure 2.4 is fundamental and relies on the use of a common multi-service IP network supporting a wide range of applications and services.

The use of IP to communicate with and control small devices and sensors opens the way for the convergence of large, IT-oriented networks with real time and specialized networked applications.

Currently, the IoT is made up of a loose collection of disparate, purpose-built networks, which are mostly not inter-connected. Today's vehicles, for example, have multiple networks to control engine function, safety features, communications systems, and so on.

Commercial and residential buildings also have various control systems for heating, venting, and air conditioning (HVAC); telephone service; security; and lighting.

As the IoT evolves, these networks, and many others, will be connected with added security, analytics, and management capabilities and some of them will converge. This will allow the IoT to become even more powerful in what

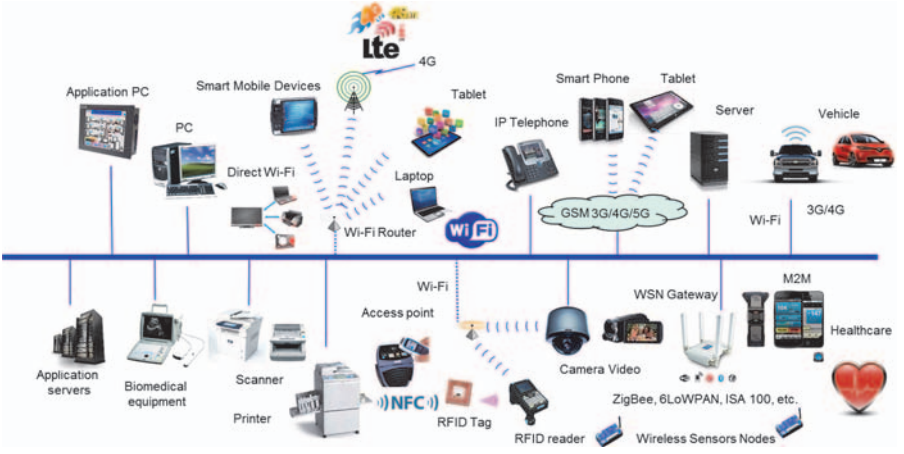

Fig. 2.4 IP convergence.

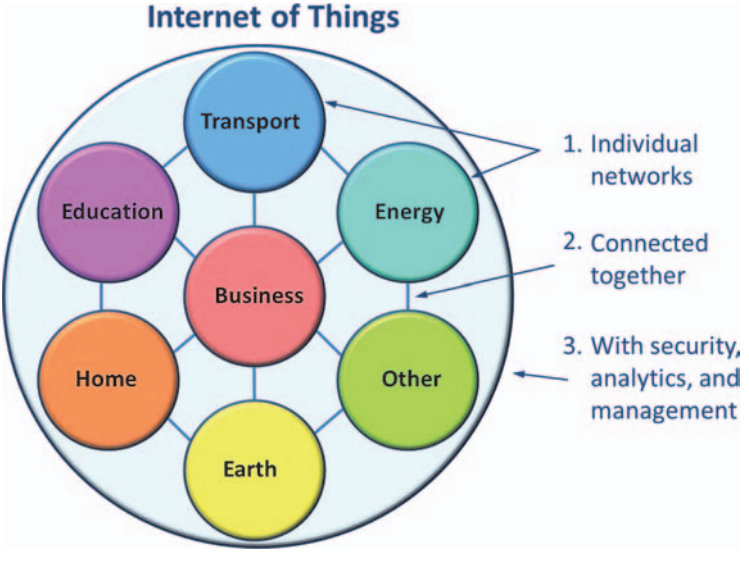

Fig. 2.5 IoT viewed as a network of networks.
(*Source*: Cisco IBSG, April 2011).

it can help people achieve [25]. A presentation of IoT as a network of networks is given in Figure 2.5.

The Internet of Things is not a single technology, it's a concept in which most new things are connected and enabled such as street lights being

networked and things like embedded sensors, image recognition functionality, augmented reality, and near field communication are integrated into situational decision support, asset management and new services. These bring many business opportunities and add to the complexity of IT [13].

Distribution, transportation, logistics, reverse logistics, field service, etc. are areas where the coupling of information and "things" may create new business processes or may make the existing ones highly efficient and more profitable.

The Internet of Things provides solutions based on the integration of information technology, which refers to hardware and software used to store, retrieve, and process data and communications technology which includes electronic systems used for communication between individuals or groups. The rapid convergence of information and communications technology is taking place at three layers of technology innovation: the cloud, data and communication pipes/networks, and device [8], as presented in Figure 2.7.

The synergy of the access and potential data exchange opens huge new possibilities for IoT applications. Already over 50% of Internet connections are between or with things. In 2011 there were over 15 billion things on the Web, with 50 billion+ intermittent connections.

By 2020, over 30 billion connected things, with over 200 billion with intermittent connections are forecast. Key technologies here include embedded sensors, image recognition and NFC. By 2015, in more than 70% of enterprises, a single executable will oversee all Internet connected things. This becomes the Internet of Everything [14].

As a result of this convergence, the IoT applications require that classical industries are adapting and the technology will create opportunities for new industries to emerge and to deliver enriched and new user experiences and services.

In addition, to be able to handle the sheer number of things and objects that will be connected in the IoT, cognitive technologies and contextual intelligence are crucial. This also applies for the development of context aware applications that need to be reaching to the edges of the network through smart devices that are incorporated into our everyday life.

The Internet is not only a network of computers, but it has evolved into a network of devices of all types and sizes, vehicles, smartphones, home appliances, toys, cameras, medical instruments and industrial systems, all

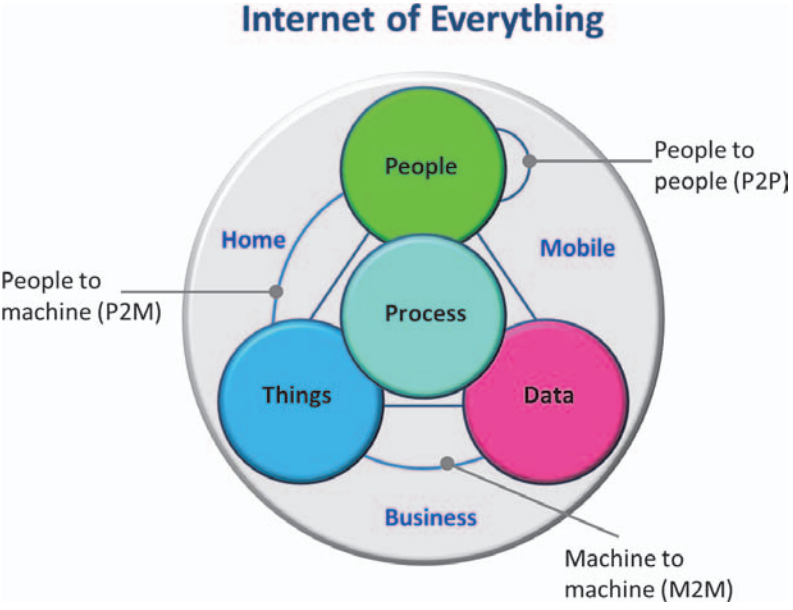

Fig. 2.6 Internet of everything.
(*Source*: Cisco).

connected, all communicating and sharing information all the time as presented in Figure 2.6.

The Internet of Things had until recently different means at different levels of abstractions through the value chain, from lower level semiconductor through the service providers.

The Internet of Things is a "global concept" and requires a common definition. Considering the wide background and required technologies, from sensing device, communication subsystem, data aggregation and pre-processing to the object instantiation and finally service provision, generating an unambiguous definition of the "Internet of Things" is non-trivial.

The IERC is actively involved in ITU-T Study Group 13, which leads the work of the International Telecommunications Union (ITU) on standards for next generation networks (NGN) and future networks and has been part of the team which has formulated the following definition [18]: "***Internet of things (IoT):*** *A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.*

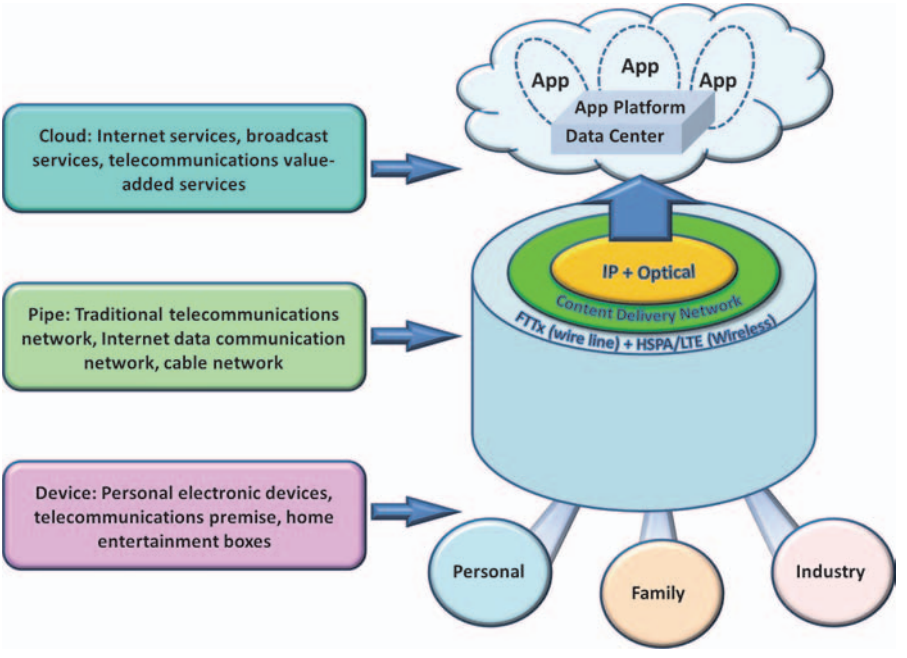

Fig. 2.7 Factors driving the convergence and contributing to the integration and transformation of cloud, pipe, and device technologies.

(*Source*: Huawei Technologies [8]).

NOTE 1 — Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled. NOTE 2 — From a broader perspective, the IoT can be perceived as a vision with technological and societal implications."

The IERC definition [19] states that IoT is "*A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.*"

2.2 IoT Strategic Research and Innovation Directions

The development of enabling technologies such as nanoelectronics, communications, sensors, smart phones, embedded systems, cloud networking, network virtualization and software will be essential to provide to things the capability

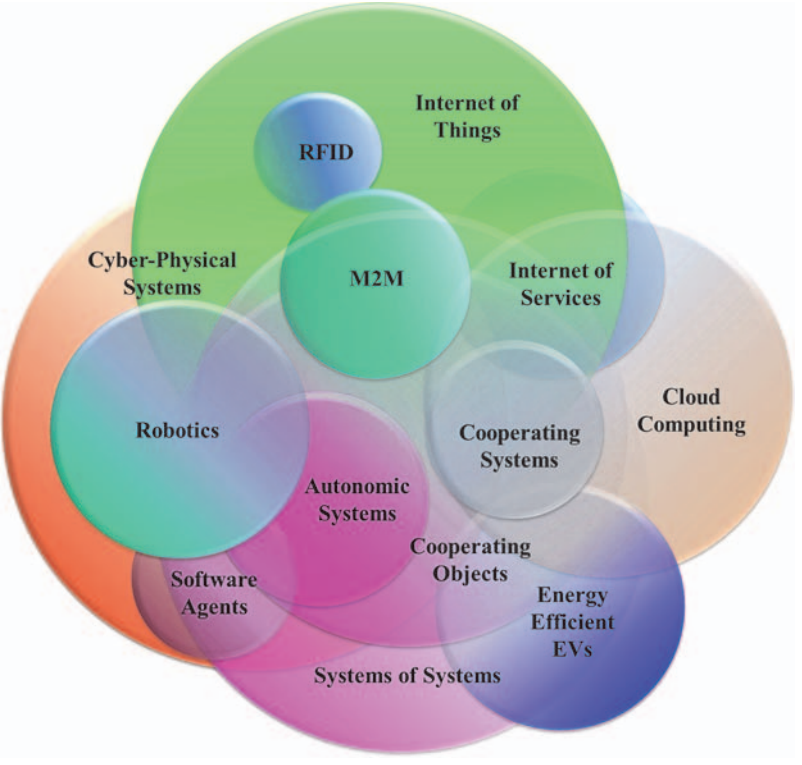

Fig. 2.8 Technology convergence.

to be connected all the time everywhere. This will also support important future IoT product innovations affecting many different industrial sectors. Some of these technologies such as embedded or cyber-physical systems form the edges of the "Internet of Things" bridging the gap between cyber space and the physical world of real "things", and are crucial in enabling the "Internet of Things" to deliver on its vision and become part of bigger systems in a world of "systems of systems". An example of technology convergence is presented in Figure 2.8.

The final report of the Key Enabling Technologies (KET), of the High-Level Expert Group [9] identified the enabling technologies, crucial to many of the existing and future value chains of the European economy:

- Nanotechnologies
- Micro and Nano electronics

- Photonics
- Biotechnology
- Advanced Materials
- Advanced Manufacturing Systems.

As such, IoT creates intelligent applications that are based on the supporting KETs identified, as IoT applications address smart environments either physical or at cyber-space level, and in real time.

To this list of key enablers, we can add the global deployment of IPv6 across the World enabling a global and ubiquitous addressing of any communicating smart thing.

From a technology perspective, the continuous increase in the integration density proposed by Moore's Law was made possible by a dimensional scaling: in reducing the critical dimensions while keeping the electrical field constant, one obtained at the same time a higher speed and a reduced power consumption of a digital MOS circuit: these two parameters became driving forces of the microelectronics industry along with the integration density.

The International Technology Roadmap for Semiconductors has emphasized in its early editions the "miniaturization" and its associated benefits in terms of performances, the traditional parameters in Moore's Law. This trend for increased performances will continue, while performance can always be traded against power depending on the individual application, sustained by the incorporation into devices of new materials, and the application of new transistor concepts. This direction for further progress is labelled "More Moore".

The second trend is characterized by functional diversification of semiconductor-based devices. These non-digital functionalities do contribute to the miniaturization of electronic systems, although they do not necessarily scale at the same rate as the one that describes the development of digital functionality. Consequently, in view of added functionality, this trend may be designated "More-than-Moore" [11].

Mobile data traffic is projected to double each year between now and 2015 and mobile operators will find it increasingly difficult to provide the bandwidth requested by customers. In many countries there is no additional spectrum that can be assigned and the spectral efficiency of mobile networks is reaching its physical limits. Proposed solutions are the seamless integration of existing Wi-Fi networks into the mobile ecosystem. This will have a direct impact on Internet of Things ecosystems.

The chips designed to accomplish this integration are known as "multicom" chips. Wi-Fi and baseband communications are expected to converge in three steps:

- 3G — the applications running on the mobile device decide which data are handled via 3G network and which are routed over the Wi-Fi network.
- LTE release eight — calls for seamless movement of all IP traffic between 3G and Wi-Fi connections.
- LTE release ten — traffic is supposed to be routed simultaneously over 3G and Wi-Fi networks.

To allow for such seamless handovers between network types, the architecture of mobile devices is likely to change and the baseband chip is expected to take control of the routing so the connectivity components are connected to the baseband or integrated in a single silicon package. As a result of this architecture change, an increasing share of the integration work is likely done by baseband manufacturers (ultra -low power solutions) rather than by handset producers.

The market for wireless communications is one of the fastest-growing segments in the integrated circuit industry. Breathtakingly fast innovation, rapid changes in communications standards, the entry of new players, and the evolution of new market sub segments will lead to disruptions across the industry. LTE and multicom solutions increase the pressure for industry consolidation, while the choice between the ARM and x86 architectures forces players to make big bets that may or may not pay off [16].

Integrated networking, information processing, sensing and actuation capabilities allow physical devices to operate in changing environments. Tightly coupled cyber and physical systems that exhibit high level of integrated intelligence are referred to as cyber-physical systems. These systems are part of the enabling technologies for Internet of Things applications where computational and physical processes of such systems are tightly interconnected and coordinated to work together effectively, with or without the humans in the loop. An example of enabling technologies for the Internet of Things is presented in Figure 2.9. Robots, intelligent buildings, implantable medical devices, vehicles that drive themselves or planes that automatically fly in a controlled airspace, are examples of cyber-physical systems that could be part of Internet of Things ecosystems.

Fig. 2.9 Internet of Things — enabling technologies.

Today many European projects and initiatives address Internet of Things technologies and knowledge. Given the fact that these topics can be highly diverse and specialized, there is a strong need for integration of the individual results. Knowledge integration, in this context is conceptualized as the process through which disparate, specialized knowledge located in multiple projects across Europe is combined, applied and assimilated.

The Strategic Research and Innovation Agenda (SRIA) is the result of a discussion involving the projects and stakeholders involved in the IERC activities, which gather the major players of the European ICT landscape addressing IoT technology priorities that are crucial for the competitiveness of European industry.

IERC Strategic Research and Innovation Agenda covers the important issues and challenges for the Internet of Things technology. It provides the vision and the roadmap for coordinating and rationalizing current and future research and development efforts in this field, by addressing the different enabling technologies covered by the Internet of Things concept and paradigm.

The Strategic Research and Innovation Agenda is developed with the support of a European-led community of interrelated projects and their stakeholders, dedicated to the innovation, creation, development and use of the Internet of Things technology.

Since the release of the first version of the Strategic Research and Innovation Agenda, we have witnessed active research on several IoT topics. On the one hand this research filled several of the gaps originally identified in the Strategic Research and Innovation Agenda, whilst on the other it created new challenges and research questions. Furthermore, recent advances in pertinent areas such as cloud computing, autonomic computing, and social networks have changed the scope of the Internet of Thing's convergence even more so. The Cluster has a goal to provide an updated document each year that records the relevant changes and illustrates emerging challenges. The updated release of this Strategic Research and Innovation Agenda builds incrementally on previous versions [19, 29] and highlights the main research topics that are associated with the development of IoT enabling technologies, infrastructures and applications with an outlook towards 2020 [22].

The research items introduced will pave the way for innovative applications and services that address the major economic and societal challenges underlined in the EU 2020 Digital Agenda [23]. In addition to boosting the development of emerging architectures and services, the directions of the Strategic Research and Innovation Agenda will collectively enable the formation of ecosystems for open innovation based on Internet of Things technologies.

The IERC Strategic Research and Innovation Agenda is developed incrementally based on its previous versions and focus on the new challenges being identified in the last period.

The updated release of the Strategic Research and Innovation Agenda is highlighting the main research topics that are associated with the development of IoT infra-structures and applications, with an outlook towards 2020 [22].

The timeline of the Internet of Things Strategic Research and Innovation Agenda covers the current decade with respect to research and the following years with respect to implementation of the research results. Of course, as the Internet and its current key applications show, we anticipate unexpected trends will emerge leading to unforeseen and unexpected development paths.

The Cluster has involved experts working in industry, research and academia to provide their vision on IoT research challenges, enabling technologies and the key applications, which are expected to arise from the current vision of the Internet of Things.

The IoT Strategic Research and Innovation Agenda covers in a logical manner the vision, the technological trends, the applications, the technology enablers, the research agenda, timelines, priorities, and finally summarises in two tables the future technological developments and research needs.

Advances in embedded sensors, processing and wireless connectivity are bringing the power of the digital world to objects and places in the physical world. IoT Strategic Research and Innovation Agenda is aligned with the findings of the 2011 Hype Cycle developed by Gartner [24], which includes the broad trend of the Internet of Things (called the "real-world Web" in earlier Gartner research.

The field of the Internet of Things is based on the paradigm of supporting the IP protocol to all edges of the Internet and on the fact that at the edge of the network many (very) small devices are still unable to support IP protocol stacks. This means that solutions centred on minimum Internet of Things devices are considered as an additional Internet of Things paradigm *without IP to all access edges*, due to their importance for the development of the field.

2.2.1 Applications and Scenarios of Relevance

The IERC vision is that "the major objectives for IoT are the creation of smart environments/spaces and self-aware things (for example: smart transport, products, cities, buildings, rural areas, energy, health, living, etc.) for climate, food, energy, mobility, digital society and health applications" [19], see Figures 2.10 and 2.11.

The outlook for the future is the emerging of a network of interconnected uniquely identifiable objects and their virtual representations in an Internet alike structure that is positioned over a network of interconnected computers allowing for the creation of a new platform for economic growth.

Smart is the new green as defined by Frost & Sullivan [12] and the green products and services will be replaced by smart products and services. Smart products have a real business case, can typically provide energy and efficiency savings of up to 30 per cent, and generally deliver a two- to three-year return

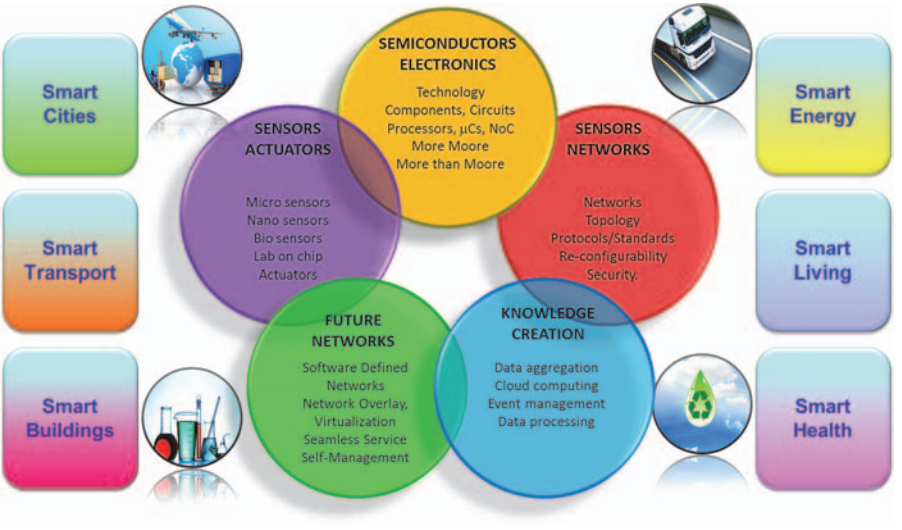

Fig. 2.10 Internet of Things — smart environments and smart spaces creation.

on investment. This trend will help the deployment of Internet of Things applications and the creation of smart environments and spaces. An illustration of Smart World is presented in Figure 2.12.

At the city level, the integration of technology and quicker data analysis will lead to a more coordinated and effective civil response to security and safety (law enforcement and blue light services); higher demand for outsourcing security capabilities.

At the building level, security technology will be integrated into systems and deliver a return on investment to the end-user through leveraging the technology in multiple applications (HR and time and attendance, customer behaviour in retail applications etc.).

There will be an increase in the development of "Smart" vehicles which have low (and possibly zero) emissions. They will also be connected to infrastructure. Additionally, auto manufacturers will adopt more use of "Smart" materials.

Intelligent packaging will be a "green" solution in its own right, reducing food waste. Intelligent materials will be used to create more comfortable clothing fabrics. Phase-change materials will help regulate temperatures in buildings, reducing energy demand for heating and cooling. Increasing investment

Fig. 2.11 Internet of Things in the context of smart environments and applications [28].

in research and development, alliances with scientific bodies and value creation with IP & product line will lead to replacement of synthetic additives by natural ingredients and formulation of fortified & enriched foods in convenient and tasty formats. Local sourcing of ingredients will become more common as the importance of what consumers eat increases. Revealing the carbon foot print of foods will be a focus in the future.

The key focus will be to make the city smarter by optimizing resources, feeding its inhabitants by urban farming, reducing traffic congestion, providing more services to allow for faster travel between home and various destinations, and increasing accessibility for essential services. It will become essential to have intelligent security systems to be implemented at key junctions in the city. Various types of sensors will have to be used to make this a reality. Sensors are moving from “smart” to “intelligent”. Biometrics is expected to be integrated with CCTV at highly sensitive locations around the city. National

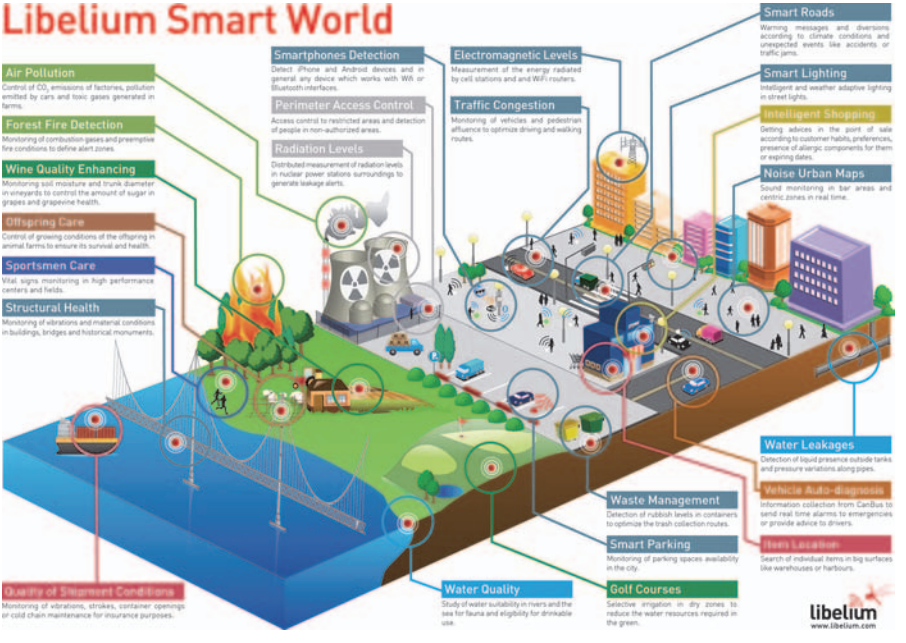

Fig. 2.12 Smart world illustration.
(*Source*: Libelium [32]).

identification cards will also become an essential tool for the identification of an individual. In addition, smart cities in 2020 will require real time auto identification security systems.

A range of smart products and concepts will significantly impact the power sector. For instance, sensors in the home will control lights, turning them off periodically when there is no movement in the room. Home Area Networks will enable utilities or individuals to control when appliances are used, resulting in a greater ability for the consumer to determine when they want to use electricity, and at what price. This is expected to equalize the need for peak power, and spread the load more evenly over time. The reduction in the need for peaking power plant capacity will help delay investment for utilities. Pattern recognizing smart meters will both help to store electricity, and pre-empt usual consumption patterns within the home. All appliances will be used as electricity storage facilities, as well as users of it. Storm water management and smart grid water will see growth.

Wastewater treatment plants will evolve into bio-refineries. New, innovative wastewater treatment processes will enable water recovery to help close the growing gap between water supply and demand.

Self-sensing controls and devices will mark new innovations in the Building Technologies space. Customers will demand more automated, self-controlled solutions with built in fault detection and diagnostic capabilities.

Development of smart implantable chips that can monitor and report individual health status periodically will see rapid growth.

Smart pumps and smart appliances/devices are expected to be significant contributors towards efficiency improvement. Process equipment with in built "smartness" to self-assess and generate reports on their performance, enabling efficient asset management, will be adopted. In the future batteries will recharge from radio signals, cell phones will recharge from Wi-Fi. Smaller Cells (micro, pico, femto) will result in more cell sites with less distance apart but they will be greener, provide power/cost savings and at the same time, higher throughput. Connected homes will enable consumers to manage their energy, media, security and appliances; will be part of the IoT applications in the future.

Test and measurement equipment is expected to become smarter in the future in response to the demand for modular instruments having lower power consumption. Furthermore, electronics manufacturing factories will become more sustainable with renewable energy and sell unused energy back to the grid, improved water conservation with rain harvesting and implement other smart building technologies, thus making their sites "Intelligent Manufacturing Facilities".

General Electric Co. considers that this is taking place through the convergence of the global industrial system with the power of advanced computing, analytics, low-cost sensing and new levels of connectivity permitted by the Internet. The deeper meshing of the digital world with the world of machines holds the potential to bring about profound transformation to global industry, and in turn to many aspects of daily life [15]. The Industrial Internet starts with embedding sensors and other advanced instrumentation in an array of machines from the simple to the highly complex, as seen in Figure 2.13. This allows the collection and analysis of an enormous amount of data, which can be used to improve machine performance, and inevitably the efficiency of the systems and networks that link them. Even the data itself can become "intelligent," instantly knowing which users it needs to reach.

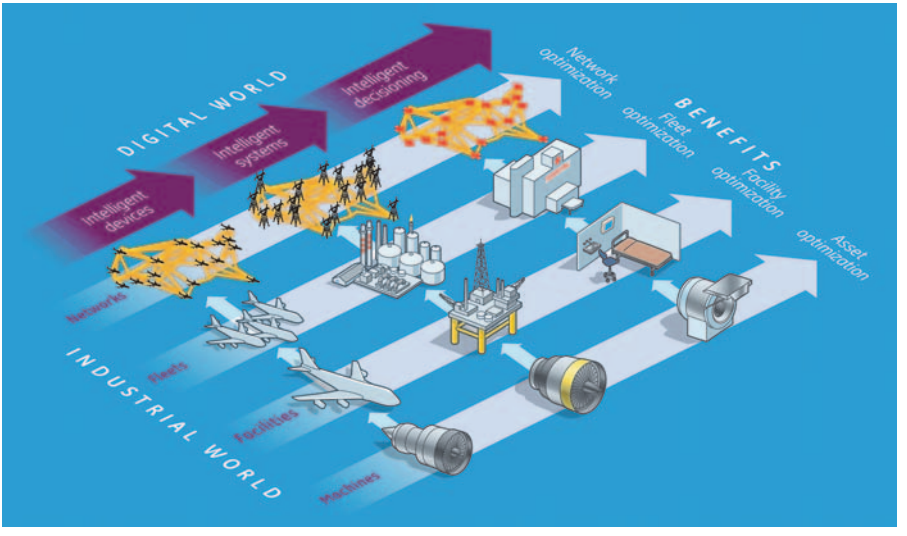

Fig. 2.13 Industrial internet applications [15].

In this context the new concept of Internet of Energy requires web based architectures to readily guarantee information delivery on demand and to change the traditional power system into a networked Smart Grid that is largely automated, by applying greater intelligence to operate, enforce policies, monitor and self-heal when necessary. This requires the integration and interfacing of the power grid to the network of data represented by the Internet, embracing energy generation, transmission, delivery, substations, distribution control, metering and billing, diagnostics, and information systems to work seamlessly and consistently.

This concept would enable the ability to produce, store and efficiently use energy, while balancing the supply/demand by using a cognitive Internet of Energy that harmonizes the energy grid by processing the data, information and knowledge via the Internet. In fact, as seen in Figure 2.14 [28], the Internet of Energy will leverage on the information highway provided by the Internet to link computers, devices and services with the distributed smart energy grid that is the freight highway for renewable energy resources allowing stakeholders to invest in green technologies and sell excess energy back to the utility.

The Internet of Energy applications are connected through the Future Internet and Internet of Things enabling seamless and secure interactions and

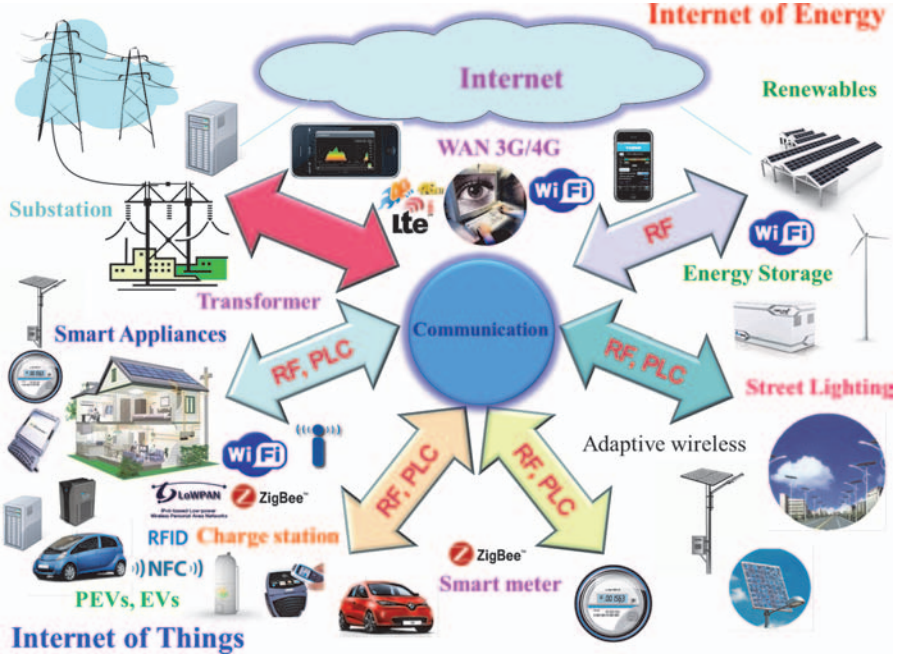

Fig. 2.14 Internet of Things embedded in internet of energy applications [28].

cooperation of intelligent embedded systems over heterogeneous communication infrastructures [28].

It is expected that this "development of smart entities will encourage development of the novel technologies needed to address the emerging challenges of public health, aging population, environmental protection and climate change, conservation of energy and scarce materials, enhancements to safety and security and the continuation and growth of economic prosperity." The IoT applications are further linked with Green ICT, as the IoT will drive energy-efficient applications such as smart grid, connected electric cars, energy-efficient buildings, thus eventually helping in building green intelligent cities.

2.2.2 IoT Functional View

The Internet of Things concept refers to uniquely identifiable things with their virtual representations in an Internet-like structure and IoT solutions

comprising a number of components such as:

- Module for interaction with local IoT devices (for example embedded in a mobile phone or located in the immediate vicinity of the user and thus contactable via a short range wireless interface). This module is responsible for acquisition of observations and their forwarding to remote servers for analysis and permanent storage.
- Module for local analysis and processing of observations acquired by IoT devices.
- Module for interaction with remote IoT devices, directly over the Internet or more likely via a proxy. This module is responsible for acquisition of observations and their forwarding to remote servers for analysis and permanent storage.
- Module for application specific data analysis and processing. This module is running on an application server serving all clients. It is taking requests from mobile and web clients and relevant IoT observations as input, executes appropriate data processing algorithms and generates output in terms of knowledge that is later presented to users.
- Module for integration of IoT-generated information into the business processes of an enterprise. This module will be gaining importance with the increased use of IoT data by enterprises as one of the important factors in day-to-day business or business strategy definition.
- User interface (web or mobile): visual representation of measurements in a given context (for example on a map) and interaction with the user, i.e. definition of user queries.

It is important to highlight that one of the crucial factors for the success of IoT is stepping away from vertically-oriented, closed systems towards open systems, based on open APIs and standardized protocols at various system levels.

In this context innovative architecture and platforms are needed to support highly complex and inter-connected IoT applications. A key consideration is how to enable development and application of comprehensive architectural frameworks that include both the physical and cyber elements based on

enabling technologies. In addition, considering the technology convergence trend, new platforms will be needed for communication and to effectively extract actionable information from vast amounts of raw data, while providing a robust timing and systems framework to support the real-time control and synchronization requirements of complex, networked, engineered physical/cyber/virtual systems.

A large number of applications made available through application markets have significantly helped the success of the smart phone industry. The development of such a huge number of smart phone applications is primarily due to involvement of the developers' community at large. Developers leveraged smart phone open platforms and the corresponding development tools, to create a variety of applications and to easily offer them to a growing number of users through the application markets.

Similarly, an IoT ecosystem has to be established, defining open APIs for developers and offering appropriate channels for delivery of new applications. Such open APIs are of particular importance on the level of the module for application specific data analysis and processing, thus allowing application developers to leverage the underlying communication infrastructure and use and combine information generated by various IoT devices to produce new, added value.

Although this might be the most obvious level at which it is important to have open APIs, it is equally important to aim towards having such APIs defined on all levels in the system. At the same time one should have in mind the heterogeneity and diversity of the IoT application space. This will truly support the development of an IoT ecosystem that encourages development of new applications and new business models.

The complete system will have to include supporting tools providing security and business mechanisms to enable interaction between a numbers of different business entities that might exist [30].

Research challenges:

- Design of open APIs on all levels of the IoT ecosystem
- Design of standardized formats for description of data generated by IoT devices to allow mashups of data coming from different domains and/or providers.

2.2.3 Application Areas

In the last few years the evolution of markets and applications, and therefore their economic potential and their impact in addressing societal trends and challenges for the next decades has changed dramatically. Societal trends are grouped as: health and wellness, transport and mobility, security and safety, energy and environment, communication and e-society, as presented in Figure 2.15. These trends create significant opportunities in the markets of consumer electronics, automotive electronics, medical applications, communication, etc. The applications in these areas benefit directly by the More-Moore and More-than-Moore semiconductor technologies, communications, networks, and software developments.

Potential applications of the IoT are numerous and diverse, permeating into practically all areas of every-day life of individuals (the so-called "smart life"), enterprises, and society as a whole. The 2010 Internet of Things Strategic Research Agenda (SRA) [19] has identified and described the main Internet of Things applications, which span numerous applications — that can be

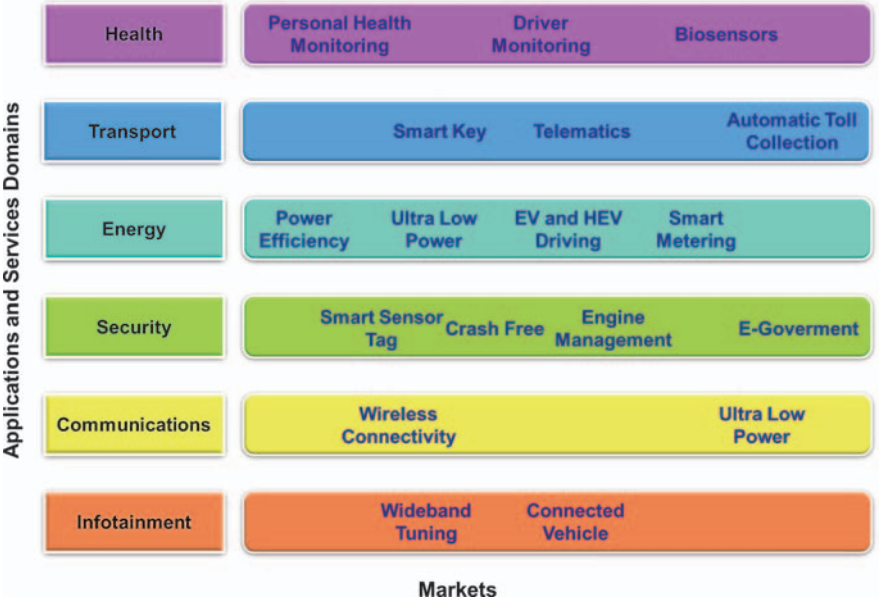

Fig. 2.15 Application matrix: Societal needs vs. market segments.

often referred to as "vertical" — domains: smart energy, smart health, smart buildings, smart transport, smart living and smart city. The vision of a pervasive IoT requires the integration of the various vertical domains (mentioned before) into a single, unified, horizontal domain which is often referred to as smart life.

The IoT application domains identified by IERC [19, 29] are based on inputs from experts, surveys [31] and reports [32]. The IoT application covers "smart" environments/spaces in domains such as: Transportation, Building, City, Lifestyle, Retail, Agriculture, Factory, Supply chain, Emergency, Health care, User interaction, Culture and Tourism, Environment and Energy.

The applications areas include as well the domain of Industrial Internet [15] where intelligent devices, intelligent systems, and intelligent decision-making represent the primary ways in which the physical world of machines, facilities, fleets and networks can more deeply merge with the connectivity, big data and analytics of the digital world as represented in Figure 2.16.

The updated list presented below, includes examples of IoT applications in different domains, which is showing why the Internet of Things is one of the strategic technology trends for the next 5 years.

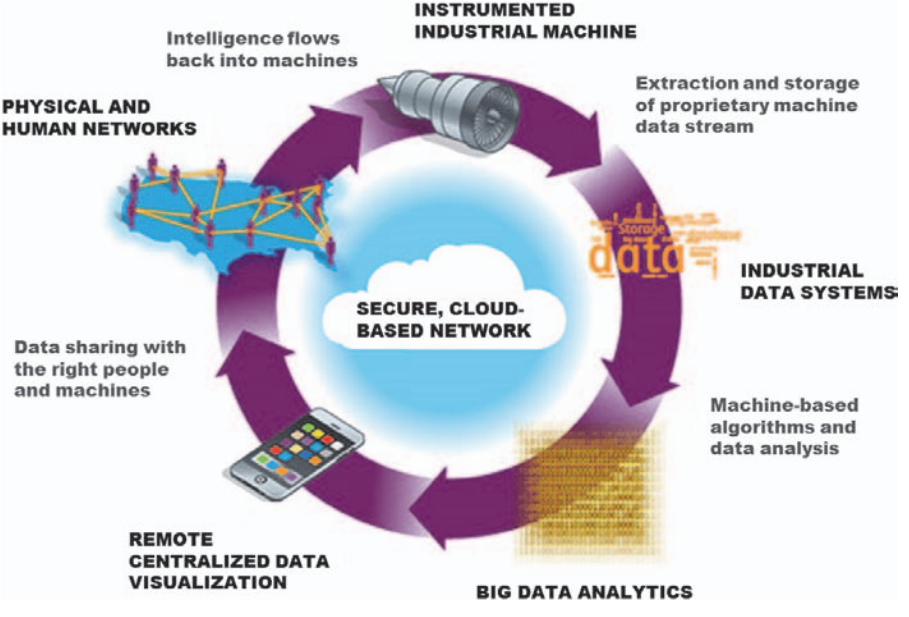

Fig. 2.16 Industrial Internet Data Loop [15].

Cities

Smart Parking: Monitoring of parking spaces availability in the city.

Structural health: Monitoring of vibrations and material conditions in buildings, bridges and historical monuments.

Noise Urban Maps: Sound monitoring in bar areas and centric zones in real time.

Traffic Congestion: Monitoring of vehicles and pedestrian levels to optimize driving and walking routes.

Smart Lightning: Intelligent and weather adaptive lighting in street lights.

Waste Management: Detection of rubbish levels in containers to optimize the trash collection routes.

Intelligent Transportation Systems: Smart Roads and Intelligent Highways with warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams.

Environment

Forest Fire Detection: Monitoring of combustion gases and preemptive fire conditions to define alert zones.

Air Pollution: Control of CO_2 emissions of factories, pollution emitted by cars and toxic gases generated in farms.

Landslide and Avalanche Prevention: Monitoring of soil moisture, vibrations and earth density to detect dangerous patterns in land conditions.

Earthquake Early Detection: Distributed control in specific places of tremors.

Water

Water Quality: Study of water suitability in rivers and the sea for fauna and eligibility for drinkable use.

Water Leakages: Detection of liquid presence outside tanks and pressure variations along pipes.

River Floods: Monitoring of water level variations in rivers, dams and reservoirs.

Energy Smart Grid, Smart Metering

Smart Grid: Energy consumption monitoring and management.

Tank level: Monitoring of water, oil and gas levels in storage tanks and cisterns.

Photovoltaic Installations: Monitoring and optimization of performance in solar energy plants.

Water Flow: Measurement of water pressure in water transportation systems.

Silos Stock Calculation: Measurement of emptiness level and weight of the goods.

Security & Emergencies

Perimeter Access Control: Access control to restricted areas and detection of people in non-authorized areas.

Liquid Presence: Liquid detection in data centres, warehouses and sensitive building grounds to prevent break downs and corrosion.

Radiation Levels: Distributed measurement of radiation levels in nuclear power stations surroundings to generate leakage alerts.

Explosive and Hazardous Gases: Detection of gas levels and leakages in industrial environments, surroundings of chemical factories and inside mines.

Retail

Supply Chain Control: Monitoring of storage conditions along the supply chain and product tracking for traceability purposes.

NFC Payment: Payment processing based in location or activity duration for public transport, gyms, theme parks, etc.

Intelligent Shopping Applications: Getting advice at the point of sale according to customer habits, preferences, presence of allergic components for them or expiring dates.

Smart Product Management: Control of rotation of products in shelves and warehouses to automate restocking processes.

Logistics

Quality of Shipment Conditions: Monitoring of vibrations, strokes, container openings or cold chain maintenance for insurance purposes.

Item Location: Search of individual items in big surfaces like warehouses or harbours.

Storage Incompatibility Detection: Warning emission on containers storing inflammable goods closed to others containing explosive material.

Fleet Tracking: Control of routes followed for delicate goods like medical drugs, jewels or dangerous merchandises.

Industrial Control

M2M Applications: Machine auto-diagnosis and assets control.

Indoor Air Quality: Monitoring of toxic gas and oxygen levels inside chemical plants to ensure workers and goods safety.

Temperature Monitoring: Control of temperature inside industrial and medical fridges with sensitive merchandise.

Ozone Presence: Monitoring of ozone levels during the drying meat process in food factories.

Indoor Location: Asset indoor location by using active (ZigBee, UWB) and passive tags (RFID/NFC).

Vehicle Auto-diagnosis: Information collection from CAN Bus to send real time alarms to emergencies or provide advice to drivers.

Agriculture

Wine Quality Enhancing: Monitoring soil moisture and trunk diameter in vineyards to control the amount of sugar in grapes and grapevine health.

Green Houses: Control micro-climate conditions to maximize the production of fruits and vegetables and its quality.

Golf Courses: Selective irrigation in dry zones to reduce the water resources required in the green.

Meteorological Station Network: Study of weather conditions in fields to forecast ice formation, rain, drought, snow or wind changes.

Compost: Control of humidity and temperature levels in alfalfa, hay, straw, etc. to prevent fungus and other microbial contaminants.

Animal Farming

Offspring Care: Control of growing conditions of the offspring in animal farms to ensure its survival and health.

Animal Tracking: Location and identification of animals grazing in open pastures or location in big stables.

Toxic Gas Levels: Study of ventilation and air quality in farms and detection of harmful gases from excrements.

Domotic & Home Automation

Energy and Water Use: Energy and water supply consumption monitoring to obtain advice on how to save cost and resources.

Remote Control Appliances: Switching on and off remotely appliances to avoid accidents and save energy.

Intrusion Detection Systems: Detection of window and door openings and violations to prevent intruders.

Art and Goods Preservation: Monitoring of conditions inside museums and art warehouses.

eHealth

Fall Detection: Assistance for elderly or disabled people living independent.

Medical Fridges: Control of conditions inside freezers storing vaccines, medicines and organic elements.

Sportsmen Care: Vital signs monitoring in high performance centres and fields.

Patients Surveillance: Monitoring of conditions of patients inside hospitals and in old people's home.

Ultraviolet Radiation: Measurement of UV sun rays to warn people not to be exposed in certain hours.

The IoT application space is very diverse and IoT applications serve different users. Different user categories have different driving needs. From the IoT perspective there are three important user categories:

- The individual citizens,
- Community of citizens (citizens of a city, a region, country or society as a whole), and
- The enterprises.

Examples of the individual citizens/human users' needs for the IoT applications are as follows:

- To increase their safety or the safety of their family members — for example remotely controlled alarm systems, or activity detection for elderly people;
- To make it possible to execute certain activities in a more convenient manner — for example: a personal inventory reminder;
- To generally improve life-style — for example monitoring health parameters during a workout and obtaining expert's advice based on the findings, or getting support during shopping;
- To decrease the cost of living — for example building automation that will reduce energy consumption and thus the overall cost.

The society as a user has different drivers. It is concerned with issues of importance for the whole community, often related to medium to longer term challenges.

Some of the needs driving the society as a potential user of IoT are the following:

- To ensure public safety — in the light of various recent disasters such as the nuclear catastrophe in Japan, the tsunami in the Indian Ocean, earthquakes, terrorist attacks, etc. One of the crucial concerns of the society is to be able to predict such events as far ahead as possible and to make rescue missions and recovery as efficient as possible. One good example of an application of IoT technology was during the Japan nuclear catastrophe, when numerous Geiger counters owned by individuals were connected to the Internet to provide a detailed view of radiation levels across Japan.
- To protect the environment
    - Requirements for reduction of carbon emissions have been included in various legislations and agreements aimed at reducing the impact on the planet and making sustainable development possible.
    - Monitoring of various pollutants in the environment, in particular in the air and in the water.

    - Waste management, not just general waste, but also electrical devices and various dangerous goods are important and challenging topics in every society.
    - Efficient utilization of various energy and natural resources are important for the development of a country and the protection of its resources.
- To create new jobs and ensure existing ones are sustainable — these are important issues required to maintain a high level quality of living.

Enterprises, as the third category of IoT users have different needs and different drivers that can potentially push the introduction of IoT-based solutions.

Examples of the needs are as follows:

- Increased productivity — this is at the core of most enterprises and affects the success and profitability of the enterprise;
- Market differentiation — in a market saturated with similar products and solutions, it is important to differentiate, and IoT is one of the possible differentiators;
- Cost efficiency — reducing the cost of running a business is a "mantra" for most of the CEOs. Better utilization of resources, better information used in the decision process or reduced downtime are some of the possible ways to achieve this.

The explanations of the needs of each of these three categories are given from a European perspective. To gain full understanding of these issues, it is important to capture and analyse how these needs are changing across the world. With such a complete picture, we will be able to drive IoT developments in the right direction.

Another important topic which needs to be understood is the business rationale behind each application. In other words, understanding the value an application creates.

Important research questions are: who takes the cost of creating that value; what are the revenue models and incentives for participating, using or contributing to an application? Again due to the diversity of the IoT application domain and different driving forces behind different applications, it will not

be possible to define a universal business model. For example, in the case of applications used by individuals, it can be as straightforward as charging a fee for a service, which will improve their quality of life. On the other hand, community services are more difficult as they are fulfilling needs of a larger community. While it is possible that the community as a whole will be willing to pay (through municipal budgets), we have to recognise the limitations in public budgets, and other possible ways of deploying and running such services have to be investigated.

2.3 IoT Applications

It is impossible to envisage all potential IoT applications having in mind the development of technology and the diverse needs of potential users. In the following sections, we present several applications, which are important. These applications are described, and the research challenges are identified. The IoT applications are addressing the societal needs and the advancements to enabling technologies such as nanoelectronics and cyber-physical systems continue to be challenged by a variety of technical (i.e., scientific and engineering), institutional, and economical issues.

The list is limited to the applications chosen by the IERC as priorities for the next years and it provides the research challenges for these applications. While the applications themselves might be different, the research challenges are often the same or similar.

2.3.1 Smart Cities

By 2020 we will see the development of Mega city corridors and networked, integrated and branded cities. With more than 60 percent of the world population expected to live in urban cities by 2025, urbanization as a trend will have diverging impacts and influences on future personal lives and mobility. Rapid expansion of city borders, driven by increase in population and infrastructure development, would force city borders to expand outward and engulf the surrounding daughter cities to form mega cities, each with a population of more than 10 million. By 2023, there will be 30 mega cities globally, with 55 percent in developing economies of India, China, Russia and Latin America [12].

This will lead to the evolution of smart cities with eight smart features, including Smart Economy, Smart Buildings, Smart Mobility, Smart Energy,

Smart Information Communication and Technology, Smart Planning, Smart Citizen and Smart Governance. There will be about 40 smart cities globally by 2025.

The role of the cities governments will be crucial for IoT deployment. Running of the day-to-day city operations and creation of city development strategies will drive the use of the IoT. Therefore, cities and their services represent an almost ideal platform for IoT research, taking into account city requirements and transferring them to solutions enabled by IoT technology.

In Europe, the largest smart city initiatives completely focused on IoT is undertaken by the FP7 Smart Santander project [20]. This project aims at deploying an IoT infrastructure comprising thousands of IoT devices spread across several cities (Santander, Guildford, Luebeck and Belgrade). This will enable simultaneous development and evaluation of services and execution of various research experiments, thus facilitating the creation of a smart city environment.

Similarly, the OUTSMART [33] project, one of the FI PPP projects, is focusing on utilities and environment in the cities and addressing the role of IoT in waste and water management, public lighting and transport systems as well as environment monitoring.

A vision of the smart city as "horizontal domain" is proposed by the BUTLER project [34], in which many vertical scenarios are integrated and concur to enable the concept of smart life. An illustrative example is depicted in the storyline of Figure 2.17. The figure depicts several commons actions that may take place in the smart day, highlighting in each occasion which domain applies. Obviously such a horizontal scenario implies the use of heterogeneous underlying communication technologies and imposes the user to interact with various seamless and pervasive IoT services.

In this context there are numerous important research challenges for smart city IoT applications:

- Overcoming traditional silo based organization of the cities, with each utility responsible for their own closed world. Although not technological, this is one of the main barriers
- Creating algorithms and schemes to describe information created by sensors in different applications to enable useful exchange of information between different city services

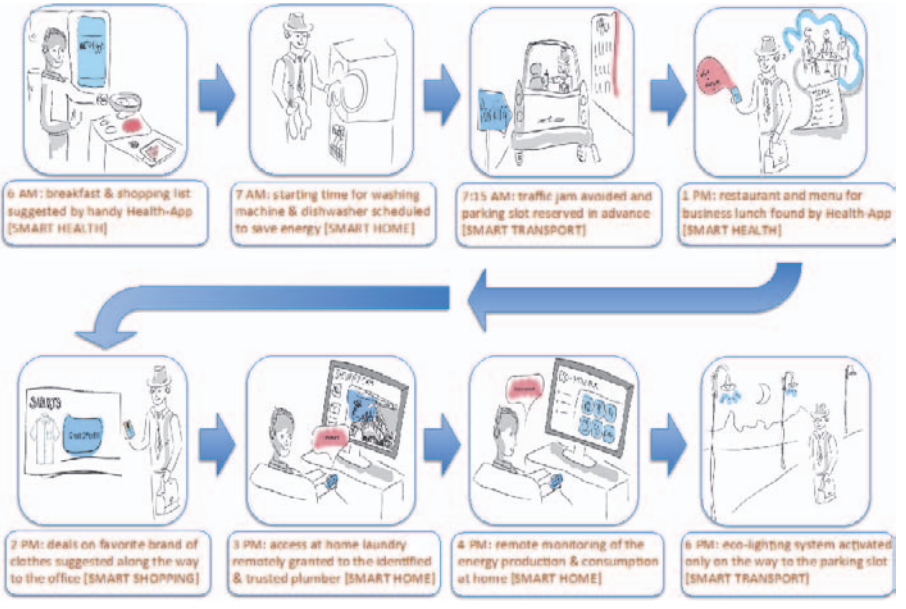
6 AM: breakfast & shopping list suggested by handy Health-App [SMART HEALTH]
7 AM: starting time for washing machine & dishwasher scheduled to save energy [SMART HOME]
7:15 AM: traffic jam avoided and parking slot reserved in advance [SMART TRANSPORT]
1 PM: restaurant and menu for business lunch found by Health-App [SMART HEALTH]
2 PM: deals on favorite brand of clothes suggested along the way to the office [SMART SHOPPING]
3 PM: access at home laundry remotely granted to the identified & trusted plumber [SMART HOME]
4 PM: remote monitoring of the energy production & consumption at home [SMART HOME]
6 PM: eco-lighting system activated only on the way to the parking slot [SMART TRANSPORT]

Fig. 2.17 A day in the life of a typical European citizen of a smart city. (*Source*: Swisscom, [34]).

- Mechanisms for cost efficient deployment and even more important maintenance of such installations, including energy scavenging
- Ensuring reliable readings from a plethora of sensors and efficient calibration of a large number of sensors deployed everywhere from lamp-posts to waste bins
- Low energy protocols and algorithms
- Algorithms for analysis and processing of data acquired in the city and making "sense" out of it.
- IoT large scale deployment and integration

2.3.2 Smart Energy and the Smart Grid

There is increasing public awareness about the changing paradigm of our policy in energy supply, consumption and infrastructure. For several reasons our future energy supply should no longer be based on fossil resources. Neither is nuclear energy a future proof option. In consequence future energy supply needs to be based largely on various renewable resources. Increasingly focus

must be directed to our energy consumption behaviour. Because of its volatile nature such supply demands an intelligent and flexible electrical grid which is able to react to power fluctuations by controlling electrical energy sources (generation, storage) and sinks (load, storage) and by suitable reconfiguration. Such functions will be based on networked intelligent devices (appliances, micro-generation equipment, infrastructure, consumer products) and grid infrastructure elements, largely based on IoT concepts. Although this ideally requires insight into the instantaneous energy consumption of individual loads (e.g. devices, appliances or industrial equipment) information about energy usage on a per-customer level is a suitable first approach.

Future energy grids are characterized by a high number of distributed small and medium sized energy sources and power plants which may be combined virtually ad hoc to virtual power plants; moreover in the case of energy outages or disasters certain areas may be isolated from the grid and supplied from within by internal energy sources such as photovoltaics on the roofs, block heat and power plants or energy storages of a residential area ("islanding").

A grand challenge for enabling technologies such as cyber-physical systems is the design and deployment of an energy system infrastructure that is able to provide blackout free electricity generation and distribution, is flexible enough to allow heterogeneous energy supply to or withdrawal from the grid, and is impervious to accidental or intentional manipulations. Integration of cyber-physical systems engineering and technology to the existing electric grid and other utility systems is a challenge. The increased system complexity poses technical challenges that must be considered as the system is operated in ways that were not intended when the infrastructure was originally built. As technologies and systems are incorporated, security remains a paramount concern to lower system vulnerability and protect stakeholder data [27]. These challenges will need to be address as well by the IoT applications that integrate heterogeneous cyber-physical systems.

The developing Smart Grid, which is represented in Figure 2.18, is expected to implement a new concept of transmission network which is able to efficiently route the energy which is produced from both concentrated and distributed plants to the final user with high security and quality of supply standards. Therefore the Smart Grid is expected to be the implementation of a kind of "Internet" in which the energy packet is managed similarly to the data packet — across routers and gateways which autonomously can decide the best

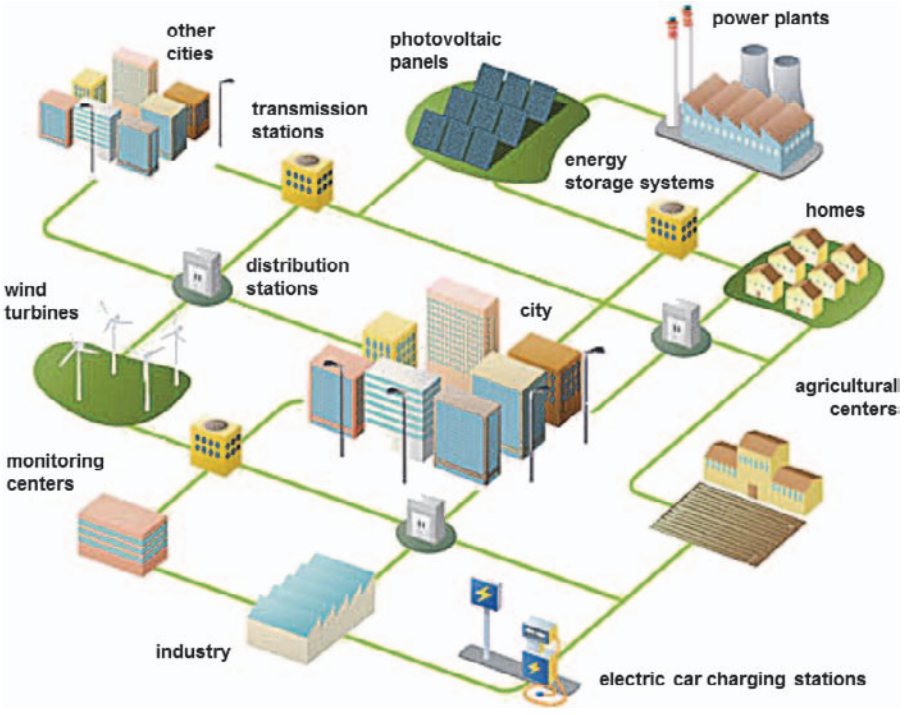

Fig. 2.18 Smart grid representation.

pathway for the packet to reach its destination with the best integrity levels. In this respect the "Internet of Energy" concept is defined as a network infrastructure based on standard and interoperable communication transceivers, gateways and protocols that will allow a real time balance between the local and the global generation and storage capability with the energy demand. This will also allow a high level of consumer awareness and involvement. The Internet of Energy (IoE) provides an innovative concept for power distribution, energy storage, grid monitoring and communication as presented in Figure 2.19. It will allow units of energy to be transferred when and where it is needed. Power consumption monitoring will be performed on all levels, from local individual devices up to national and international level [44].

Saving energy based on an improved user awareness of momentary energy consumption is another pillar of future energy management concepts. Smart meters can give information about the instantaneous energy consumption to

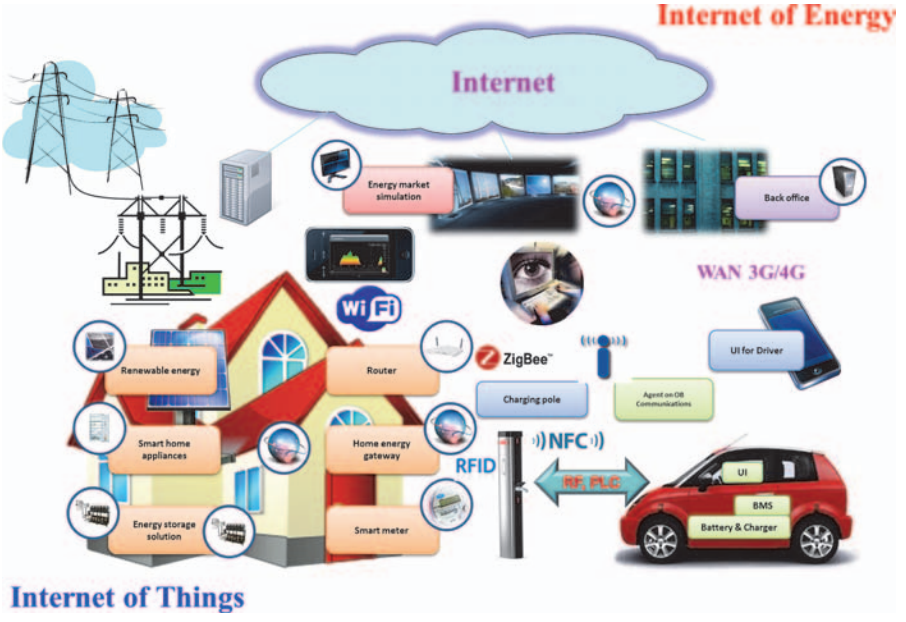

Fig. 2.19 Internet of energy: Residential building ecosystem [44].

the user, thus allowing for identification and elimination of energy wasting devices and for providing hints for optimizing individual energy consumption. In a smart grid scenario energy consumption will be manipulated by a volatile energy price which again is based on the momentary demand (acquired by smart meters) and the available amount of energy and renewable energy production. In a virtual energy marketplace software agents may negotiate energy prices and place energy orders to energy companies. It is already recognised that these decisions need to consider environmental information such as weather forecasts, local and seasonal conditions. These must be to a much finer time scale and spatial resolution.

In the long run electro mobility will become another important element of smart power grids. An example of electric mobility ecosystem is presented in Figure 2.20. Electric vehicles (EVs) might act as a power load as well as moveable energy storage linked as IoT elements to the energy information grid (smart grid). IoT enabled smart grid control may need to consider energy demand and offerings in the residential areas and along the major roads based on traffic forecast. EVs will be able to act as sink or source of energy based on

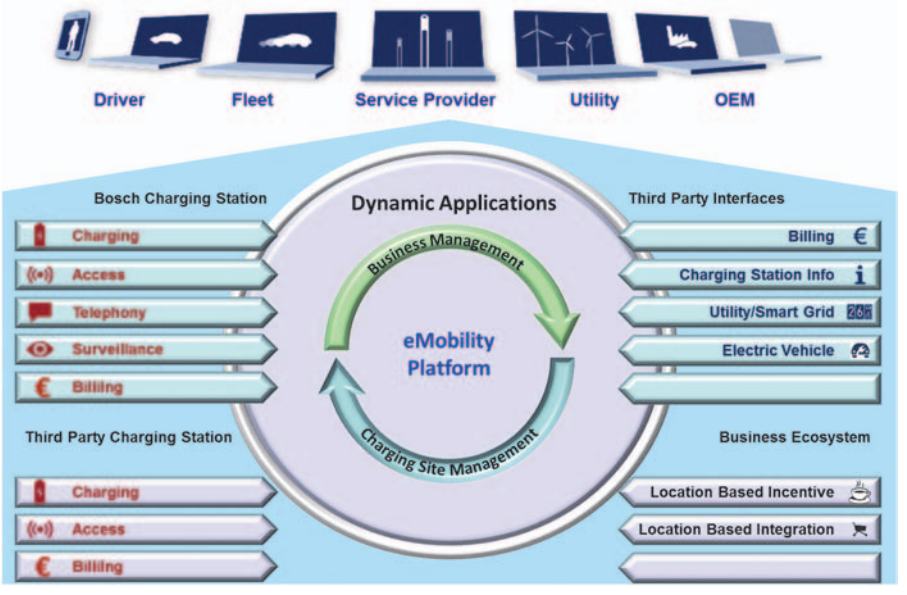

Fig. 2.20 Electric mobility ecosystem.
(*Source*: Bosch).

their charge status, usage schedule and energy price which again may depend on abundance of (renewable) energy in the grid. This is the touch point from where the following telematics IoT scenarios will merge with smart grid IoT.

This scenario is based on the existence of an IoT network of a vast multitude of intelligent sensors and actuators which are able to communicate safely and reliably. Latencies are critical when talking about electrical control loops. Even though not being a critical feature, low energy dissipation should be mandatory. In order to facilitate interaction between different vendors' products the technology should be based on a standardized communication protocol stack. When dealing with a critical part of the public infrastructure, data security is of the highest importance. In order to satisfy the extremely high requirements on reliability of energy grids, the components as well as their interaction must feature the highest reliability performance.

New organizational and learning strategies for sensor networks will be needed in order to cope with the shortcomings of classical hierarchical control concepts. The intelligence of smart systems does not necessarily need to be built into the devices at the systems' edges. Depending on connectivity,

cloud-based IoT concepts might be advantageous when considering energy dissipation and hardware effort.

Sophisticated and flexible data filtering, data mining and processing procedures and systems will become necessary in order to handle the high amount of raw data provided by billions of data sources. System and data models need to support the design of flexible systems which guarantee a reliable and secure real-time operation.

Some research challenges:

- Absolutely safe and secure communication with elements at the network edge
- Addressing scalability and standards interoperability
- Energy saving robust and reliable smart sensors/actuators
- Technologies for data anonymity addressing privacy concerns
- Dealing with critical latencies, e.g. in control loops
- System partitioning (local/cloud based intelligence)
- Mass data processing, filtering and mining; avoid flooding of communication network
- Real-time Models and design methods describing reliable interworking of heterogeneous systems (e.g. technical/economical/social/environmental systems). Identifying and monitoring critical system elements. Detecting critical overall system states in due time
- System concepts which support self-healing and containment of damage; strategies for failure contingency management
- Scalability of security functions
- Power grids have to be able to react correctly and quickly to fluctuations in the supply of electricity from renewable energy sources such as wind and solar facilities.

2.3.3 Smart Transportation and Mobility

The connection of vehicles to the Internet gives rise to a wealth of new possibilities and applications which bring new functionalities to the individuals and/or the making of transport easier and safer. In this context the concept of Internet of Vehicles (IoV) [44] connected with the concept of Internet of

Energy (IoE) represent future trends for smart transportation and mobility applications.

At the same time creating new mobile ecosystems based on trust, security and convenience to mobile/contactless services and transportation applications will ensure security, mobility and convenience to consumer-centric transactions and services.

Representing human behaviour in the design, development, and operation of cyber physical systems in autonomous vehicles is a challenge. Incorporating human-in-the-loop considerations is critical to safety, dependability, and predictability. There is currently limited understanding of how driver behaviour will be affected by adaptive traffic control cyber physical systems. In addition, it is difficult to account for the stochastic effects of the human driver in a mixed traffic environment (i.e., human and autonomous vehicle drivers) such as that found in traffic control cyber physical systems. Increasing integration calls for security measures that are not physical, but more logical while still ensuring there will be no security compromise. As cyber physical systems become more complex and interactions between components increases, safety and security will continue to be of paramount importance [27]. All these elements are of the paramount importance for the IoT ecosystems developed based on these enabling technologies. An example of standalone energy ecosystem is presented in Figure 2.21.

When talking about IoT in the context of automotive and telematics, we may refer to the following application scenarios:

- Standards must be defined regarding the charging voltage of the power electronics, and a decision needs to be made as to whether the recharging processes should be controlled by a system within the vehicle or one installed at the charging station.
- Components for bidirectional operations and flexible billing for electricity need to be developed if electric vehicles are to be used as electricity storage media.
- **IoT as an inherent part of the vehicle control and management system**: Already today certain technical functions of the vehicles' on-board systems can be monitored on line by the service centre or garage to allow for preventative maintenance, remote diagnostics, instantaneous support and timely availability of spare parts. For

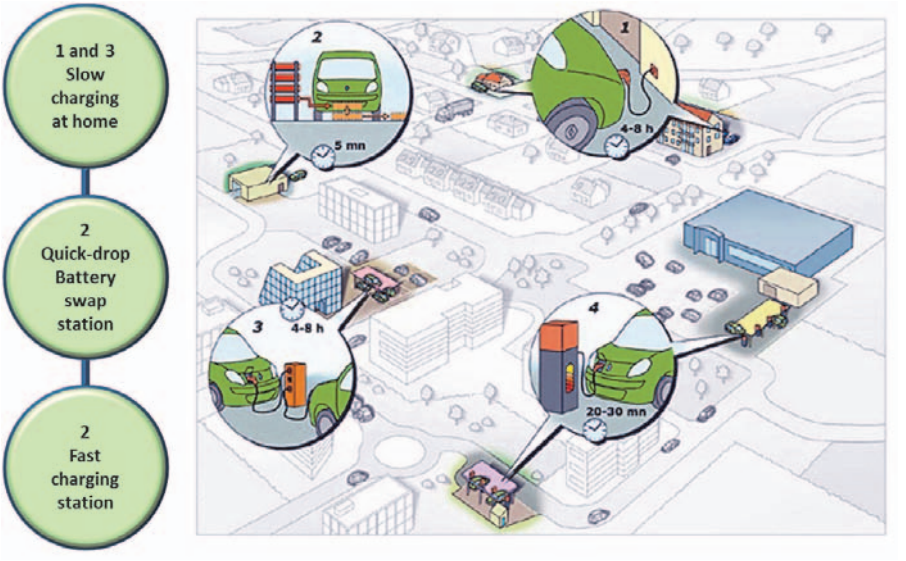

Fig. 2.21 Standalone energy ecosystem.
(*Source*: Renault Nissan).

this purpose data from on-board sensors are collected by a smart on-board unit and communicated via the Internet to the service centre.

- **IoT enabling traffic management and control**: Cars should be able to organise themselves in order to avoid traffic jams and to optimise drive energy usage. This may be done in coordination and cooperation with the infrastructure of a smart city's traffic control and management system. Additionally dynamic road pricing and parking tax can be important elements of such a system. Further mutual communications between the vehicles and with the infrastructure enable new methods for considerably increasing traffic safety, thus contributing to the reduction in the number of traffic accidents.
- **IoT enabling new transport scenarios (multi-modal transport):** In such scenarios, e.g. automotive OEMs see themselves as mobility providers rather than manufacturers of vehicles. The user will be offered an optimal solution for transportation from A to B, based on all available and suitable transport means. Thus, based on the

momentary traffic situation an ideal solution may be a mix of individual vehicles, vehicle sharing, railway, and commuter systems. In order to allow for seamless usage and on-time availability of these elements (including parking space), availability needs to be verified and guaranteed by online reservation and online booking, ideally in interplay with the above mentioned smart city traffic management systems.

These scenarios are, not independent from each other and show their full potential when combined and used for different applications. Figure 2.22 presents a communication ecosystem based on PLC Technology.

Technical elements of such systems are smart phones and smart vehicle onboard units which acquire information from the user (e.g. position, destination and schedule) and from on board systems (e.g. vehicle status, position, energy usage profile, driving profile). They interact with external systems (e.g. traffic control systems, parking management, vehicle sharing managements, electric vehicle charging infrastructure). Moreover they need to initiate and perform the related payment procedures.

Smart sensors in the road and traffic control infrastructures need to collect information about road and traffic status, weather conditions, etc. This requires

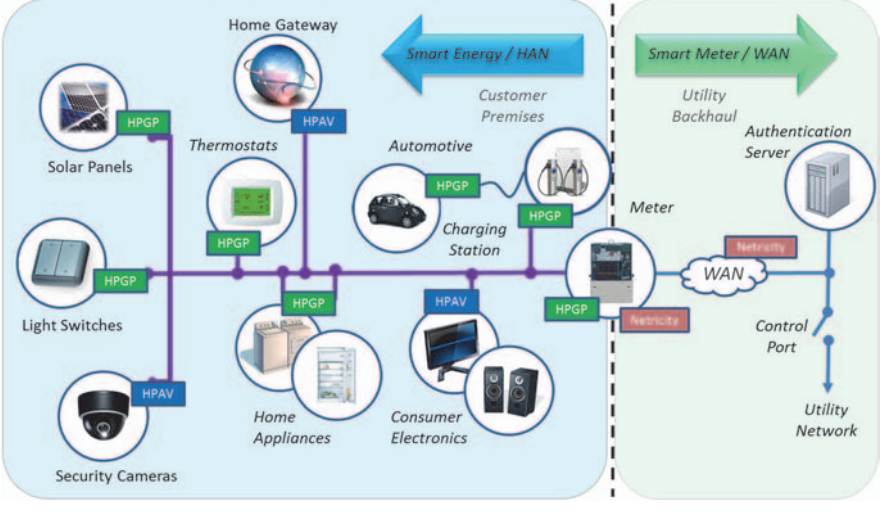

Fig. 2.22 Communication Ecosystem based on PLC Technology.
(*Source*: STM).

robust sensors (and actuators) which are able to reliably deliver information to the systems mentioned above. Such reliable communication needs to be based on M2M communication protocols which consider the timing, safety, and security constraints. The expected high amount of data will require sophisticated data mining strategies. Overall optimisation of traffic flow and energy usage may be achieved by collective organisation among the individual vehicles. First steps could be the gradual extension of DATEX-II by IoT related technologies and information. The (international) standardisation of protocol stacks and interfaces is of utmost importance to enable economic competition and guarantee smooth interaction of different vendor products.

When dealing with information related to individuals' positions, destinations, schedules, and user habits, privacy concerns gain highest priority. They even might become road blockers for such technologies. Consequently not only secure communication paths but also procedures which guarantee anonymity and de-personalization of sensible data are of interest.

Some research challenges:

- Safe and secure communication with elements at the network edge, inter-vehicle communication, and vehicle to infrastructure communication
- Energy saving robust and reliable smart sensors and actuators in vehicles and infrastructure
- Technologies for data anonymity addressing privacy concerns
- System partitioning (local/cloud based intelligence)
- Identifying and monitoring critical system elements. Detecting critical overall system states in due time
- Technologies supporting self-organisation and dynamic formation of structures/re-structuring
- Ensure an adequate level of trust and secure exchange of data among different vertical ICT infrastructures (e.g., intermodal scenario).

2.3.4 Smart Home, Smart Buildings and Infrastructure

The rise of Wi-Fi's role in home automation has primarily come about due to the networked nature of deployed electronics where electronic devices (TVs and AV receivers, mobile devices, etc.) have started becoming part of the

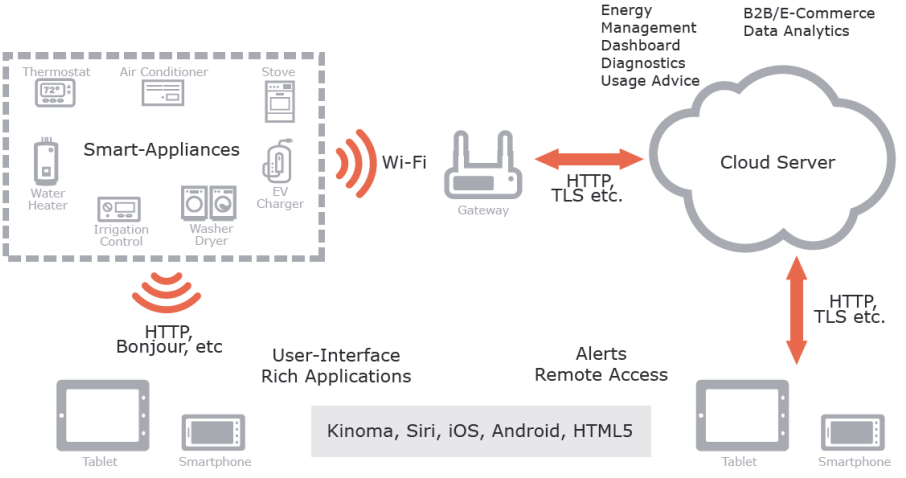

Fig. 2.23 Smart_home_platform.
(*Source*: Marvell).

home IP network and due the increasing rate of adoption of mobile computing devices (smartphones, tablets, etc.), see Figure 2.23. The networking aspects are bringing online streaming services or network playback, while becoming a mean to control of the device functionality over the network. At the same time mobile devices ensure that consumers have access to a portable 'controller' for the electronics connected to the network. Both types of devices can be used as gateways for IoT applications. In this context many companies are considering building platforms that integrate the building automation with entertainment, healthcare monitoring, energy monitoring and wireless sensor monitoring in the home and building environments.

IoT applications using sensors to collect information about operating conditions combined with cloud hosted analytics software that analyse disparate data points will help facility managers become far more proactive about managing buildings at peak efficiency.

Issues of building ownership (i.e., building owner, manager, or occupants) challenge integration with questions such as who pays initial system cost and who collects the benefits over time. A lack of collaboration between the subsectors of the building industry slows new technology adoption and can prevent new buildings from achieving energy, economic and environmental performance targets.

Integration of cyber physical systems both within the building and with external entities, such as the electrical grid, will require stakeholder cooperation to achieve true interoperability. As in all sectors, maintaining security will be a critical challenge to overcome [27].

Within this field of research the exploitation of the potential of wireless sensor networks (WSNs) to facilitate intelligent energy management in buildings, which increases occupant comfort while reducing energy demand, is highly relevant. In addition to the obvious economic and environmental gains from the introduction of such intelligent energy management in buildings other positive effects will be achieved. Not least of which is the simplification of building control; as placing monitoring, information feedback equipment and control capabilities in a single location will make a buildings' energy management system easier to handle for the building owners, building managers, maintenance crews and other users of the building. Using the Internet together with energy management systems also offers an opportunity to access a buildings' energy information and control systems from a laptop or a Smartphone placed anywhere in the world. This has a huge potential for providing the managers, owners and inhabitants of buildings with energy consumption feedback and the ability to act on that information.

In the context of the future Internet of Things, Intelligent Building Management Systems can be considered part of a much larger information system. This system is used by facilities managers in buildings to manage energy use and energy procurement and to maintain buildings systems. It is based on the infrastructure of the existing Intranets and the Internet, and therefore utilises the same standards as other IT devices. Within this context reductions in the cost and reliability of WSNs are transforming building automation, by making the maintenance of energy efficient healthy productive work spaces in buildings increasingly cost effective [21].

2.3.5 Smart Factory and Smart Manufacturing

The role of the Internet of Things is becoming more prominent in enabling access to devices and machines, which in manufacturing systems, were hidden in well-designed silos. This evolution will allow the IT to penetrate further the digitized manufacturing systems. The IoT will connect the factory to a whole

new range of applications, which run around the production. This could range from connecting the factory to the smart grid, sharing the production facility as a service or allowing more agility and flexibility within the production systems themselves. In this sense, the production system could be considered one of the many Internets of Things (IoT), where a new ecosystem for smarter and more efficient production could be defined.

The first evolutionary step towards a shared smart factory could be demonstrated by enabling access to today's external stakeholders in order to interact with an IoT-enabled manufacturing system. These stakeholders could include the suppliers of the productions tools (e.g. machines, robots), as well as the production logistics (e.g. material flow, supply chain management), and maintenance and re-tooling actors. An IoT-based architecture that challenges the hierarchical and closed factory automation pyramid, by allowing the above-mentioned stakeholders to run their services in multiple tier flat production system is proposed in [140]. This means that the services and applications of tomorrow do not need to be defined in an intertwined and strictly linked manner to the physical system, but rather run as services in a shared physical world. The room for innovation in the application space could be increased in the same degree of magnitude as this has been the case for embedded applications or Apps, which have exploded since the arrival of smart phones (i.e. the provision of a clear and well standardized interface to the embedded hardware of a mobile phone to be accessed by all types of Apps).

One key enabler to this ICT-driven smart and agile manufacturing lies in the way we manage and access the physical world, where the sensors, the actuators, and also the production unit should be accessed, and managed in the same or at least similar IoT standard interfaces and technologies. These devices are then providing their services in a well-structured manner, and can be managed and orchestrated for a multitude of applications running in parallel.

The convergence of microelectronics and micromechanical parts within a sensing device, the ubiquity of communications, the rise of micro-robotics, the customization made possible by software will significantly change the world of manufacturing. In addition, broader pervasiveness of telecommunications in many environments is one of the reasons why these environments take the shape of ecosystems.

Some of the main challenges associated with the implementation of cyber-physical systems include affordability, network integration, and the interoperability of engineering systems.

Most companies have a difficult time justifying risky, expensive, and uncertain investments for smart manufacturing across the company and factory level. Changes to the structure, organization, and culture of manufacturing occur slowly, which hinders technology integration. Pre-digital age control systems are infrequently replaced because they are still serviceable. Retrofitting these existing plants with cyber-physical systems is difficult and expensive. The lack of a standard industry approach to production management results in customized software or use of a manual approach. There is also a need for a unifying theory of non-homogeneous control and communication systems [27].

2.3.6 Smart Health

The market for health monitoring devices is currently characterised by application-specific solutions that are mutually non-interoperable and are made up of diverse architectures. While individual products are designed to cost targets, the long-term goal of achieving lower technology costs across current and future sectors will inevitably be very challenging unless a more coherent approach is used. An example of a smart health platform is given in Figure 2.24.

The links between the many applications in health monitoring are:

- Applications require the gathering of data from sensors
- Applications must support user interfaces and displays
- Applications require network connectivity for access to infrastructural services
- Applications have in-use requirements such as low power, robustness, durability, accuracy and reliability.

IoT applications are pushing the development of platforms for implementing ambient assisted living (AAL) systems that will offer services in the areas of assistance to carry out daily activities, health and activity monitoring, enhancing safety and security, getting access to medical and emergency systems, and facilitating rapid health support. The main objective is to enhance life quality for people who need permanent support or monitoring, to decrease

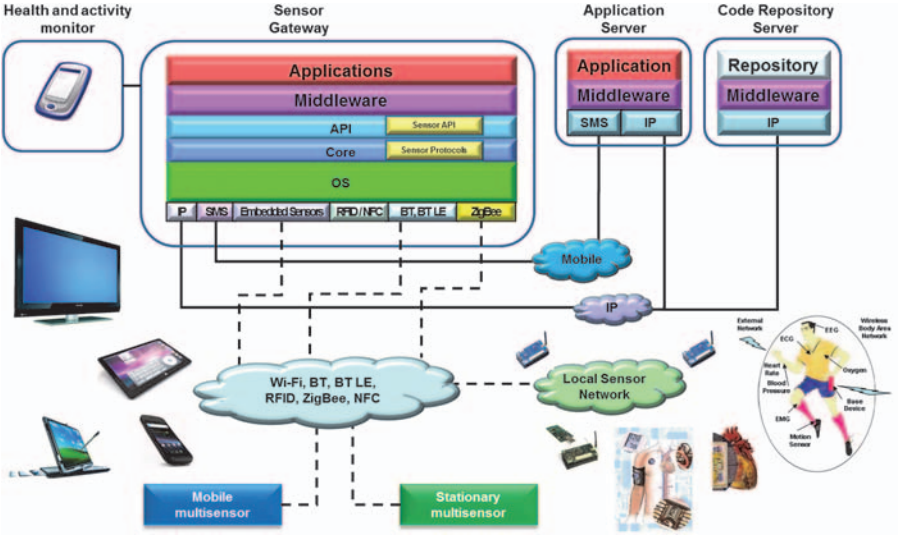

Fig. 2.24 Example of smart_health_platform.

barriers for monitoring important health parameters, to avoid unnecessary healthcare costs and efforts, and to provide the right medical support at the right time.

Challenges exist in the overall cyber-physical infrastructure (e.g., hardware, connectivity, software development and communications), specialized processes at the intersection of control and sensing, sensor fusion and decision making, security, and the compositionality of cyber-physical systems. Proprietary medical devices in general were not designed for interoperation with other medical devices or computational systems, necessitating advancements in networking and distributed communication within cyber-physical architectures. Interoperability and closed loop systems appears to be the key for success. System security will be critical as communication of individual patient data is communicated over cyber-physical networks. In addition, validating data acquired from patients using new cyber-physical technologies against existing gold standard data acquisition methods will be a challenge. Cyber-physical technologies will also need to be designed to operate with minimal patient training or cooperation [27].

New and innovative technologies are needed to cope with the trends on wired, wireless, high-speed interfaces, miniaturization and modular

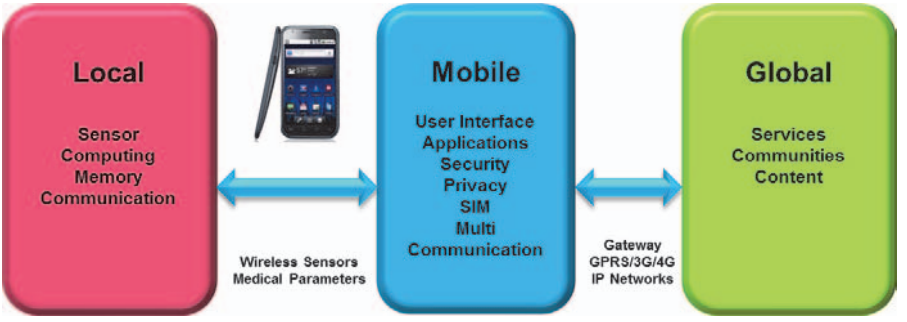

Fig. 2.25 Communication layers in smart_health_platforms.

design approaches for products having multiple technologies integrated. The communication technologies are addressing different levels and layers in the smart health platforms, as shown in Figure 2.25.

Internet of Things applications have a future market potential for electronic health services and connected telecommunication industry. In this context, the telecommunications can foster the evolution of ecosystems in different application areas. Medical expenditures are in the range of 10% of the European gross domestic product. The market segment of telemedicine, one of lead markets of the future will have growth rates of more than 19%.

Convergence of bio parameter sensing, communication technologies and engineering is turning health care into a new type of information industry. In this context the progress beyond state of the art for IoT applications for healthcare is envisaged as follows:

- Standardisation of interface from sensors and MEMS for an open platform to create a broad and open market for bio-chemical innovators.
- Providing a high degree of automation in the taking and processing of information;
- Real-time data over networks (streaming and regular single measurements) to be available to clinicians anywhere on the web with appropriate software and privileges; data travelling over trusted web.
- Reuse of components over smooth progression between low-cost "home health" devices and higher cost "professional" devices.

- Data needs to be interchangeable between all authorised devices in use within the clinical care pathway, from home, ambulance, clinic, GP, hospital, without manual transfer of data.

2.3.7 Food and Water Tracking and Security

Food and fresh water are the most important natural resources in the world. Organic food produced without addition of certain chemical substances and according to strict rules, or food produced in certain geographical areas will be particularly valued. Similarly, fresh water from mountain springs is already highly valued. In the future it will be very important to bottle and distribute water adequately. This will inevitably lead to attempts to forge the origin or the production process. Using IoT in such scenarios to secure tracking of food or water from the production place to the consumer is one of the important topics.

This has already been introduced to some extent in regard to beef meat. After the "mad cow disease" outbreak in the late 20th century, some beef manufacturers together with large supermarket chains in Ireland are offering "from pasture to plate" traceability of each package of beef meat in an attempt to assure consumers that the meat is safe for consumption. However, this is limited to certain types of food and enables tracing back to the origin of the food only, without information on the production process.

IoT applications need to have a development framework that will assure the following:

- The things connected to the Internet need to provide value. The things that are part of the IoT need to provide a valuable service at a price point that enables adoption, or they need to be part of a larger system that does.
- Use of rich ecosystem for the development. The IoT comprises things, sensors, communication systems, servers, storage, analytics, and end user services. Developers, network operators, hardware manufacturers, and software providers need to come together to make it work. The partnerships among the stakeholders will provide functionality easily available to the customers.
- Systems need to provide APIs that let users take advantage of systems suited to their needs on devices of their choice. APIs also allow

developers to innovate and create something interesting using the system's data and services, ultimately driving the system's use and adoption.

- Developers need to be attracted since the implementation will be done on a development platform. Developers using different tools to develop solutions, which work across device platforms playing a key role for future IoT deployment.
- Security needs to be built in. Connecting things previously cut off from the digital world will expose them to new attacks and challenges.

The research challenges are:

- Design of secure, tamper-proof and cost-efficient mechanisms for tracking food and water from production to consumers, enabling immediate notification of actors in case of harmful food and communication of trusted information.
- Secure way of monitoring production processes, providing sufficient information and confidence to consumers. At the same time details of the production processes which might be considered as intellectual property, should not be revealed.
- Ensure trust and secure exchange of data among applications and infrastructures (farm, packing industry, retailers) to prevent the introduction of false or misleading data, which can affect the health of the citizens or create economic damage to the stakeholders.

2.3.8 Participatory Sensing

People live in communities and rely on each other in everyday activities. Recommendations for a good restaurant, car mechanic, movie, phone plan etc. were and still are some of the things where community knowledge helps us in determining our actions.

While in the past this community wisdom was difficult to access and often based on inputs from a handful of people, with the proliferation of the web and more recently social networks, the community knowledge has become readily available — just a click away.

Today, the community wisdom is based on conscious input from people, primarily based on opinions of individuals. With the development of IoT

Fig. 2.26 Internet of Things and smart home concept.
(*Source*: IBM).

technology and ICT in general, it is becoming interesting to expand the concept of community knowledge to automated observation of events in the real world. An example of the smart home concept using Internet of Things is represented in Figure 2.26.

Smart phones are already equipped with a number of sensors and actuators: camera, microphone, accelerometers, temperature gauge, speakers, displays etc. A range of other portable sensing products that people will carry in their pockets will soon become available as well. Furthermore, our cars are equipped with a range of sensors capturing information about the car itself, and also about the road and traffic conditions.

Intel is working to simplify deployment of the Internet of Things with its Intelligent Systems Framework (Intel® ISF), a set of interoperable solutions

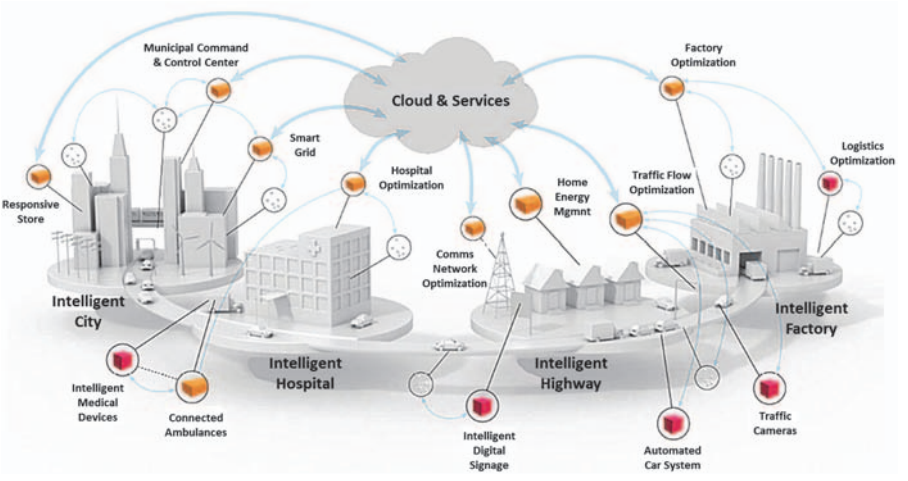

Fig. 2.27 Internet of Things: Intelligent systems framework. (*Source*: Intel).

designed to address connecting, managing, and securing devices and data in a consistent and scalable manner, as represented in Figure 2.27.

Participatory sensing applications aim at utilizing each person, mobile phone, and car and associated sensors as automatic sensory stations taking a multi-sensor snapshot of the immediate environment. By combining these individual snapshots in an intelligent manner it is possible to create a clear picture of the physical world that can be shared and for example used as an input to the smart city services decision processes.

However, participatory sensing applications come with a number of challenges that need to be solved:

- Design of algorithms for normalization of observations taking into account the conditions under which the observations were taken. For example temperature measurements will be different if taken by a mobile phone in a pocket or a mobile phone lying on a table;
- Design of robust mechanisms for analysis and processing of collected observations in real time (complex event processing) and generation of "community wisdom" that can be reliably used as an input to decision taking;
- Reliability and trustworthiness of observed data, i.e. design of mechanisms that will ensure that observations were not tampered

with and/or detection of such unreliable measurements and consequent exclusion from further processing. In this context, the proper identification and authentication of the data sources is an important function;
- Ensuring privacy of individuals providing observations;
- Efficient mechanisms for sharing and distribution of "community wisdom";
- Addressing scalability and large scale deployments.

2.3.9 Social Networks and IoT

From a user perspective, abstract connectedness and real-world interdependencies are not easily captured mentally. What users however easily relate to is the social connectedness of family and friends. The user engagement in IoT awareness could build on the Social Network paradigm, e.g. as described in [36] and [37], where the users interact with the real world entities of interest via the social network paradigm. This combination leads to interesting and popular applications (such as [38]), which will become more sophisticated and innovative.

Future research directions in IoT applications should consider the social dimension, based on integration with social networks which can be seen as another bundle of information streams. Note also that social networks are characterized by the massive participation of human users. Hence, the wave of social IoT applications is likely to be built over successful paradigms of participatory sensing applications (e.g., [39, 40, 42]), which will be extending on the basis of an increased number of autonomous interacting Internet-connected devices. The use of the social networks metaphor for the interactions between Internet-connected objects has been recently proposed [43] and it could enable novel forms of M2M, interactions and related applications.

2.4 Internet of Things and Related Future Internet Technologies

2.4.1 Cloud Computing

Since the publication of the 2011 SRA, cloud computing has been established as one of the major building blocks of the Future Internet. New technology

enablers have progressively fostered virtualisation at different levels and have allowed the various paradigms known as "Applications as a Service", "Platforms as a Service" and "Infrastructure and Networks as a Service". Such trends have greatly helped to reduce cost of ownership and management of associated virtualised resources, lowering the market entry threshold to new players and enabling provisioning of new services. With the virtualisation of objects being the next natural step in this trend, the convergence of cloud computing and Internet of Things will enable unprecedented opportunities in the IoT services arena [46].

As part of this convergence, IoT applications (such as sensor-based services) will be delivered on-demand through a cloud environment [47]. This extends beyond the need to virtualize sensor data stores in a scalable fashion. It asks for virtualization of Internet-connected objects and their ability to become orchestrated into on-demand services (such as Sensing-as-a-Service).

Moreover, generalising the serving scope of an Internet-connected object beyond the "sensing service", it is not hard to imagine virtual objects that will be integrated into the fabric of future IoT services and shared and reused in different contexts, projecting an "Object as a Service" paradigm aimed as in other virtualised resource domains) at minimising costs of ownership and maintenance of objects, and fostering the creation of innovative IoT services.

Relevant topics for the research agenda will therefore include:

- The description of requests for services to a cloud/IoT infrastructure,
- The virtualization of objects,
- Tools and techniques for optimization of cloud infrastructures subject to utility and SLA criteria,
- The investigation of
    - utility metrics and
    - (reinforcement) learning techniques that could be used for gauging on-demand IoT services in a cloud environment,
- Techniques for real-time interaction of Internet-connected objects within a cloud environment through the implementation of lightweight interactions and the adaptation of real-time operating systems.

- Access control models to ensure the proper access to the data stored in the cloud.

2.4.2 IoT and Semantic Technologies

The 2010 SRA has identified the importance of semantic technologies towards discovering devices, as well as towards achieving semantic interoperability. During the past years, semantic web technologies have also proven their ability to link related data (web-of-data concept) [48], while relevant tools and techniques have just emerged [49]. Future research on IoT is likely to embrace the concept of Linked Open Data. This could build on the earlier integration of ontologies (e.g., sensor ontologies) into IoT infrastructures and applications.

Semantic technologies will also have a key role in enabling sharing and re-use of virtual objects as a service through the cloud, as illustrated in the previous paragraph. The semantic enrichment of virtual object descriptions will realise for IoT what semantic annotation of web pages has enabled in the Semantic Web. Associated semantic-based reasoning will assist IoT users to more independently find the relevant proven virtual objects to improve the performance or the effectiveness of the IoT applications they intend to use.

2.4.3 Autonomy

Spectacular advances in technology have introduced increasingly complex and large scale computer and communication systems. Autonomic computing [50], inspired by biological systems, has been proposed as a grand challenge that will allow the systems to **self-manage** this complexity, using high-level objectives and policies defined by humans. The objective is to provide some self-x properties to the system, where x can be adaptation, organization, optimization, configuration, protection, healing, discovery, description, etc.

The Internet of Things will exponentially increase the scale and the complexity of existing computing and communication systems. **Autonomy** is thus an imperative property for IoT systems to have. However, there is still a lack of research on how to adapt and tailor existing research on autonomic computing to the specific characteristics of IoT, such as high dynamicity and distribution, real-time nature, resource constraints, and lossy environments.

2.4.3.1 Properties of Autonomic IoT Systems

The following properties are particularly important for IoT systems and need further research:

Self-adaptation

In the very dynamic context of the IoT, from the physical to the application layer, self-adaptation is an essential property that allows the communicating nodes, as well as services using them, to react in a timely manner to the continuously changing context in accordance with, for instance, business policies or performance objectives that are defined by humans. IoT systems should be able to reason autonomously and give self-adapting decisions. Cognitive radios at physical and link layers, self-organising network protocols, automatic service discovery and (re-)bindings at the application layer are important enablers for the self-adapting IoT.

Self-organization

In IoT systems — and especially in WS&ANs — it is very common to have nodes that join and leave the network spontaneously. The network should therefore be able to re-organize itself against this evolving topology. Self-organizing, energy efficient routing protocols have a considerable importance in the IoT applications in order to provide seamless data exchange throughout the highly heterogeneous networks. Due to the large number of nodes, it is preferable to consider solutions without a central control point like for instance clustering approaches. When working on self-organization, it is also very crucial to consider the energy consumption of nodes and to come up with solutions that maximize the IoT system lifespan and the communication efficiency within that system.

Self-optimisation

Optimal usage of the constrained resources (such as memory, bandwidth, processor, and most importantly, power) of IoT devices is necessary for sustainable and long-living IoT deployments. Given some high-level optimisation goals in terms of performance, energy consumption or quality of service, the system itself should perform necessary actions to attain its objectives.

Self-configuration

IoT systems are potentially made of thousands of nodes and devices such as sensors and actuators. Configuration of the system is therefore very complex and difficult to handle by hand. The IoT system should provide remote configuration facilities so that self-management applications automatically configure necessary parameters based on the needs of the applications and users. It consists of configuring for instance device and network parameters, installing/uninstalling/upgrading software, or tuning performance parameters.

Self-protection

Due to its wireless and ubiquitous nature, IoT will be vulnerable to numerous malicious attacks. As IoT is closely related to the physical world, the attacks will for instance aim at controlling the physical environments or obtaining private data. The IoT should autonomously tune itself to different levels of security and privacy, while not affecting the quality of service and quality of experience.

Self-healing

The objective of this property is to detect and diagnose problems as they occur and to immediately attempt to fix them in an autonomous way. IoT systems should monitor continuously the state of its different nodes and detect whenever they behave differently than expected. It can then perform actions to fix the problems encountered. Encounters could include re-configuration parameters or installing a software update.

Self-description

Things and resources (sensors and actuators) should be able to describe their characteristics and capabilities in an expressive manner in order to allow other communicating objects to interact with them. Adequate device and service description formats and languages should be defined, possibly at the semantic level. The existing languages should be re-adapted in order to find a trade-off between the expressiveness, the conformity and the size of the descriptions. Self-description is a fundamental property for implementing plug and play resources and devices.

Self-discovery

Together with the self-description, the self-discovery feature plays an essential role for successful IoT deployments. IoT devices/services should be dynamically discovered and used by the others in a seamless and transparent way. Only powerful and expressive device and service discovery protocols (together with description protocols) would allow an IoT system to be fully dynamic (topology-wise).

Self-matchmaking

To fully unlock the IoT potential, virtual objects will have to:

- Be reusable outside the context for which they were originally deployed and
- Be reliable in the service they provide.

On the one hand, IoT services will be able to exploit enriched availability of underlying objects. They will also have to cope with their unreliable nature and be able to find suitable "equivalent object" alternatives in case of failure, unreachability etc. Such envisaged dynamic service-enhancement environments will require self-matchmaking features (between services and objects and vice versa) that will prevent users of IoT future services from having to (re-)configure objects themselves.

Self-energy-supplying

And finally, self-energy-supplying is a tremendously important (and very IoT specific) feature to realize and deploy sustainable IoT solutions. Energy harvesting techniques (solar, thermal, vibration, etc.) should be preferred as a main power supply, rather than batteries that need to be replaced regularly, and that have a negative effect on the environment.

2.4.3.2 Research Directions for Self-manageable IoT Systems

Given the above mentioned challenges, we propose the following research directions to progress towards self-manageable IoT systems:

- Already existing fundamental research results from domains including artificial intelligence, biological systems, control theory,

embedded systems and software engineering are necessary to build scientifically-proven, solid, robust and reliable solutions. It may be necessary to tailor existing research to the IoT context. In addition, multidisciplinary conferences and workshops should be organised to foster the interaction level between experts in those domains.

- Novel methodologies, architectures, algorithms, technologies, and protocols should be developed taking into account IoT-specific characteristics such as resource constraints, dynamic, un-predictive, error prone and lossy environments, distributed and real-time data handling and decision-making requirements, etc. Characterisation of self-x properties in IoT context should be done based on real-life cross-domain use cases.
- Autonomic issues should be considered from the very early phases of IoT system implementations, from conception to deployment of devices, infrastructures and services. The self-awareness property should be included to any software module, however separated from the functional code. Hardware should be designed to be reconfigurable.
- Devices should either be able to provide management data to autonomic managers, or to have embedded intelligence to reason and act locally. Automated tools for development, deployment, and supervision of IoT devices and services should be developed.
- Prototypes should be developed at early stages in order to validate the theoretical results by measuring the overhead that autonomy can bring to IoT systems.
- IoT is expected to be composed of very heterogeneous networks, thus standard interfaces should be defined for interoperability. Specific working groups on self-management issues should be created in standardisation organisations, industrial alliances and fora on IoT. A self-organising network (SON) for LTE of 3GPP is a good initiative that should be followed by other next generation network standards.
- Model-driven approaches are solid ways to provide correctness, robustness, reliability, and dependability properties, and they have already proven their importance for the conception and development of embedded systems. In the context of IoT, they

should be extended to obtain these properties not only during design and development but also at deployment and run-time for self-adaptation.

- New modes of interaction with autonomic IoT systems that would increase the quality and experience of users are necessary, e.g., user assistance with intuitive multimodal interfaces: to monitor and control autonomic systems, to define rules and policies, and to receive important feedback in real-time.
- Various stakeholders (users, manufacturers, integrators, service providers, telecom operators, etc.) will be dynamically and concurrently involved in IoT systems; particular attention should thus be paid for resource sharing and policy conflict resolution between different actors. In addition to many existing concepts from the distributed systems domain, fundamentals of economics can also be applied to resolve these issues.
- New programming paradigms should be proposed for creating self-aware applications with the ability of self-adaption on-the-fly. The flexibility, dynamicity, modularity of the service-oriented approach (SOA) is particularly interesting. An integration of SOA with new device-oriented approaches can be useful for programming cyber-physical environments.
- Security and privacy issues should be considered very seriously since IoT deals not only with huge amounts of sensitive data (personal data, business data, etc.) but also has the power of influencing the physical environment with its control abilities. Cyber-physical environments must thus be protected from any kind of malicious attacks.
- Addressing scalability for a large scale IoT deployment is another key issue. Integration with IPv6 and global resource directories should be further researched, including collateral issues such as authentication and privacy management with distributed IoT across global networks.
- In order to make the smart objects paradigm come true (objects with perception capabilities, embedded intelligence and high level of autonomy and communication) much research is needed in order to fit sensors/actuators, CPU, memory, energy, etc. into

tiny chips. The challenge is quite high, assuming that autonomy requires complex algorithms which themselves require high CPU power and therefore also a comfortable amount of available energy.
- Self-management systems should be designed with particular attention in contexts where the safety of the user can be impacted (e.g., driving cars). In some cases, policies should be embedded in the system to prevent safety risk in case of malfunction of the self-management system.

2.4.4 Situation Awareness and Cognition

Integration of sensory, computing and communication devices (e.g. smart phones, GPS) into the Internet is becoming common. This is increasing the ability to extract "content" from the data generated and understand it from the viewpoint of the wider application domain (i.e. meta-data). This ability to extract content becomes ever more crucial and complex, especially when we consider the amount of data that is generated. Complexity can be reduced through the integration of self-management and automatic learning features (i.e. exploiting cognitive principles). The application of cognitive principles in the extraction of "content" from data can also serve as a foundation towards creating overall awareness of a current situation. This then gives a system the ability to respond to changes within its situational environment, with little or no direct instruction from users and therefore facilitate customised, dependable and reliable service creation.

2.5 Infrastructure

The Internet of Things will become part of the fabric of everyday life. It will become part of our overall infrastructure just like water, electricity, telephone, TV and most recently the Internet. Whereas the current Internet typically connects full-scale computers, the Internet of Things (as part of the Future Internet) will connect everyday objects with a strong integration into the physical world.

2.5.1 Plug and Play Integration

If we look at IoT-related technology available today, there is a huge heterogeneity. It is typically deployed for very specific purposes and the configuration

requires significant technical knowledge and may be cumbersome. To achieve a true Internet of Things we need to move away from such small-scale, vertical application silos, towards a horizontal infrastructure on which a variety of applications can run simultaneously.

This is only possible if connecting a thing to the Internet of Things becomes as simple as plugging it in and switching it on. Such plug and play functionality requires an infrastructure that supports it, starting from the networking level and going beyond it to the application level. This is closely related to the aspects discussed in the section on autonomy. On the networking level, the plug & play functionality has to enable the communication, features like the ones provided by IPv6 are in the directions to help in this process. Suitable infrastructure components have then to be discovered to enable the integration into the Internet of Things. This includes announcing the functionalities provided, such as what can be sensed or what can be actuated.

2.5.2 Infrastructure Functionality

The infrastructure needs to support applications in finding the things required. An application may run anywhere, including on the things themselves. Finding things is not limited to the start-up time of an application. Automatic adaptation is needed whenever relevant new things become available, things become unavailable or the status of things changes. The infrastructure has to support the monitoring of such changes and the adaptation that is required as a result of the changes.

2.5.3 Semantic Modelling of Things

To reach the full potential of the Internet of Things, semantic information regarding the things, the information they can provide or the actuations they can perform need to be available. It is not sufficient to know that there is a temperature sensor or an electric motor, but it is important to know which temperature the sensor measures: the indoor temperature of a room or the temperature of the fridge, and that the electric motor can open or close the blinds or move something to a different location. As it may not be possible to provide such semantic information by simply switching on the thing, the infrastructure should make adding it easy for users. Also, it may be possible to derive semantic information, given some basic information and additional

knowledge, e.g. deriving information about a room, based on the information that a certain sensor is located in the room. This should be enabled by the infrastructure.

2.5.4 Physical Location and Position

As the Internet of Things is strongly rooted in the physical world, the notion of physical location and position are very important, especially for finding things, but also for deriving knowledge. Therefore, the infrastructure has to support finding things according to location (e.g. geo-location based discovery). Taking mobility into account, localization technologies will play an important role for the Internet of Things and may become embedded into the infrastructure of the Internet of Things.

2.5.5 Security and Privacy

In addition, an infrastructure needs to provide support for security and privacy functions including identification, confidentiality, integrity, non-repudiation authentication and authorization. Here the heterogeneity and the need for interoperability among different ICT systems deployed in the infrastructure and the resource limitations of IoT devices (e.g., Nano sensors) have to be taken into account.

2.5.6 Infrastructure-related Research Questions

Based on the description above of what an infrastructure for the Internet of Things should look like, we see the following challenges and research questions:

- How can the plug and play functionality be achieved taking into account the heterogeneity of the underlying technology?
- How should the resolution and discovery infrastructure look to enable finding things efficiently?
- How can monitoring and automatic adaptation be supported by the infrastructure?
- How can semantic information be easily added and utilized within the infrastructure?

- How can new semantic information be derived from existing semantic information based on additional knowledge about the world, and how can this be supported by the infrastructure?
- How can the notion of physical location be best reflected in the infrastructure to support the required functionalities mentioned above?
- How should the infrastructure support for security and privacy look?
- How can the infrastructure support accounting and charging as the basis for different IoT business models?
- How we can provide security and privacy functions at infrastructure level on the basis of heterogeneous and resource limited components of the infrastructure?

2.6 Networks and Communication

Present communication technologies span the globe in wireless and wired networks and support global communication by globally-accepted communication standards. The Internet of Things Strategic Research and Innovation Agenda (SRIA) intends to lay the foundations for the Internet of Things to be developed by research through to the end of this decade and for subsequent innovations to be realised even after this research period. Within this time frame the number of connected devices, their features, their distribution and implied communication requirements will develop; as will the communication infrastructure and the networks being used. Everything will change significantly. Internet of Things devices will be contributing to and strongly driving this development.

Changes will first be embedded in given communication standards and networks and subsequently in the communication and network structures defined by these standards.

2.6.1 Networking Technology

The evolution and pervasiveness of present communication technologies has the potential to grow to unprecedented levels in the near future by including the world of things into the developing Internet of Things.

Network users will be humans, machines, things and groups of them.

2.6.1.1 Complexity of the Networks of the Future

A key research topic will be to understand the complexity of these future networks and the expected growth of complexity due to the growth of Internet of Things. The research results of this topic will give guidelines and timelines for defining the requirements for network functions, for network management, for network growth and network composition and variability [91].

Wireless networks cannot grow without such side effects as interference.

2.6.1.2 Growth of Wireless Networks

Wireless networks especially will grow largely by adding vast amounts of small Internet of Things devices with minimum hardware, software and intelligence, limiting their resilience to any imperfections in all their functions.

Based on the research of the growing network complexity, caused by the Internet of Things, predictions of traffic and load models will have to guide further research on unfolding the predicted complexity to real networks, their standards and on-going implementations.

Mankind is the maximum user group for the mobile phone system, which is the most prominent distributed system worldwide besides the fixed telephone system and the Internet. Obviously the number of body area networks [1, 92, 93], and of networks integrated into clothes and further personal area networks — all based on Internet of Things devices — will be of the order of the current human population. They are still not unfolding into reality. In a second stage cross network cooperative applications are likely to develop, which are not yet envisioned.

2.6.1.3 Mobile Networks

Applications such as body area networks may develop into an autonomous world of small, mobile networks being attached to their bearers and being connected to the Internet by using a common point of contact. The mobile phone of the future could provide this function.

Analysing worldwide industrial processes will be required to find limiting set sizes for the number of machines and all things being implied or used within their range in order to develop an understanding of the evolution steps to the Internet of Things in industrial environments.

2.6.1.4 Expanding Current Networks to Future Networks

Generalizing the examples given above, the trend may be to expand current end user network nodes into networks of their own or even a hierarchy of networks. In this way networks will grow on their current access side by unfolding these outermost nodes into even smaller, attached networks, spanning the Internet of Things in the future. In this context networks or even networks of networks will be mobile by themselves.

2.6.1.5 Overlay Networks

Even if network construction principles should best be unified for the world-wide Internet of Things and the networks bearing it, there will not be one unified network, but several. In some locations even multiple networks overlaying one another physically and logically.

The Internet and the Internet of Things will have access to large parts of these networks. Further sections may be only represented by a top access node or may not be visible at all globally. Some networks will by intention be shielded against external access and secured against any intrusion on multiple levels.

2.6.1.6 Network Self-organization

Wireless networks being built for the Internet of Things will show a large degree of ad-hoc growth, structure, organization, and significant change in time, including mobility. These constituent features will have to be reflected in setting them up and during their operation [94].

Self-organization principles will be applied to configuration by context sensing, especially concerning autonomous negotiation of interference management and possibly cognitive spectrum usage, by optimization of network structure and traffic and load distribution in the network, and in self-healing of networks. All will be done in heterogeneous environments, without interaction by users or operators.

2.6.1.7 IPv6, IoT and Scalability

The current transition of the global Internet to IPv6 will provide a virtually unlimited number of public IP addresses able to provide bidirectional and

symmetric (true M2M) access to Billions of smart things. It will pave the way to new models of IoT interconnection and integration. It is raising numerous questions: How can the Internet infrastructure cope with a highly heterogeneous IoT and ease a global IoT interconnection? How interoperability will happen with legacy systems? What will be the impact of the transition to IPv6 on IoT integration, large scale deployment and interoperability? It will probably require developing an IPv6-based European research infrastructure for the IoT.

2.6.1.8 Green Networking Technology

Network technology has traditionally developed along the line of predictable progress of implementation technologies in all their facets. Given the enormous expected growth of network usage and the number of user nodes in the future, driven by the Internet of Things, there is a real need to minimize the resources for implementing all network elements and the energy being used for their operation [95].

Disruptive developments are to be expected by analysing the energy requirements of current solutions and by going back to principles of communication in wired, optical and wireless information transfer. Research done by Bell Labs [96, 97] in recent years shows that networks can achieve an energy efficiency increase of a factor of 1,000 compared to current technologies [98].

The results of the research done by the GreenTouch consortium [96] should be integrated into the development of the network technologies of the future. These network technologies have to be appropriate to realise the Internet of Things and the Future Internet in their most expanded state to be anticipated by the imagination of the experts.

2.6.2 Communication Technology

2.6.2.1 Unfolding the Potential of Communication Technologies

The research aimed at communication technology to be undertaken in the coming decade will have to develop and unfold all potential communication profiles of Internet of Things devices, from bit-level communication to continuous

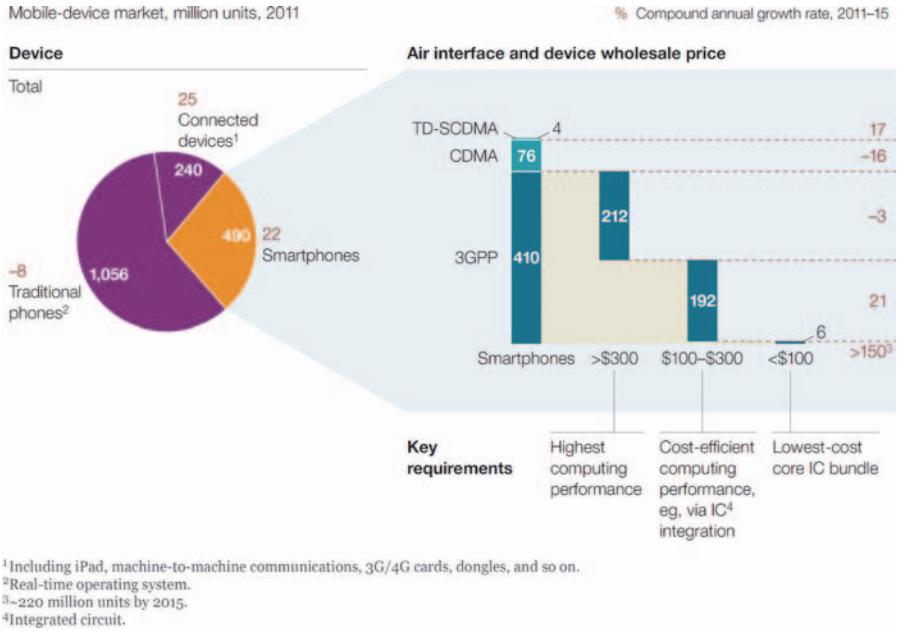

Fig. 2.28 Growth mobile device market.

(*Source*: Strategy analytics; McKinsey analysis [16]).

data streams, from sporadic connections to connections being always on, from standard services to emergency modes, from open communication to fully secured communication, spanning applications from local to global, based on single devices to globally-distributed sets of devices [99].

In this context the growth in mobile device market, shown in Figure 2.28, is pushing the deployment of Internet of Things applications where these mobile devices (smart phones, tablets, etc. are seen as gateways for wireless sensors and actuators.

Based on this research the anticipated bottlenecks in communications and in networks and services will have to be quantified using appropriate theoretical methods and simulation approaches.

Communications technologies for the Future Internet and the Internet of Things will have to avoid such bottlenecks by construction not only for a given status of development, but for the whole path to fully developed and still growing nets.

2.6.2.2 Correctness of Construction

Correctness of construction [100] of the whole system is a systematic process that starts from the small systems running on the devices up to network and distributed applications. Methods to prove the correctness of structures and of transformations of structures will be required, including protocols of communication between all levels of communication stacks used in the Internet of Things and the Future Internet.

These methods will be essential for the Internet of Things devices and systems, as the smallest devices will be implemented in hardware and many types will not be programmable. Interoperability within the Internet of Things will be a challenge even if such proof methods are used systematically.

2.6.2.3 An Unified Theoretical Framework for Communication

Communication between processes [101] running within an operating system on a single or multicore processor, communication between processes running in a distributed computer system [102], and the communication between devices and structures in the Internet of Things and the Future Internet using wired and wireless channels shall be merged into a unified minimum theoretical framework covering and including formalized communication within protocols.

In this way minimum overhead, optimum use of communication channels and best handling of communication errors should be achievable. Secure communication could be embedded efficiently and naturally as a basic service.

2.6.2.4 Energy-Limited Internet of Things Devices and their Communication

Many types of Internet of Things devices will be connected to the energy grid all the time; on the other hand a significant subset of Internet of Things devices will have to rely on their own limited energy resources or energy harvesting throughout their lifetime.

Given this spread of possible implementations and the expected importance of minimum-energy Internet of Things devices and applications, an important topic of research will have to be the search for minimum energy, minimum

computation, slim and lightweight solutions through all layers of Internet of Things communication and applications.

2.6.2.5 Challenge the Trend to Complexity

The inherent trend to higher complexity of solutions on all levels will be seriously questioned — at least with regard to minimum energy Internet of Things devices and services.

Their communication with the access edges of the Internet of Things network shall be optimized cross domain with their implementation space and it shall be compatible with the correctness of the construction approach.

2.6.2.6 Disruptive Approaches

Given these special restrictions, non-standard, but already existing ideas should be carefully checked again and be integrated into existing solutions, and disruptive approaches shall be searched and researched with high priority. This very special domain of the Internet of Things may well develop into its most challenging and most rewarding domain — from a research point of view and, hopefully, from an economical point of view as well.

2.7 Processes

The deployment of IoT technologies will significantly impact and change the way enterprises do business as well as interactions between different parts of the society, affecting many processes. To be able to reap the many potential benefits that have been postulated for the IoT, several challenges regarding the modelling and execution of such processes need to be solved in order to see wider and in particular commercial deployments of IoT [103]. The special characteristics of IoT services and processes have to be taken into account and it is likely that existing business process modelling and execution languages as well as service description languages such as USDL [106], will need to be extended.

2.7.1 Adaptive and Event-driven Processes

One of the main benefits of IoT integration is that processes become more adaptive to what is actually happening in the real world. Inherently, this is

based on events that are either detected directly or by real-time analysis of sensor data. Such events can occur at any time in the process. For some of the events, the occurrence probability is very low: one knows that they might occur, but not when or if at all. Modelling such events into a process is cumbersome, as they would have to be included into all possible activities, leading to additional complexity and making it more difficult to understand the modelled process, in particular the main flow of the process (the 80% case). Secondly, how to react to a single event can depend on the context, i.e. the set of events that have been detected previously.

Research on adaptive and event-driven processes could consider the extension and exploitation of EDA (Event Driven Architectures) for activity monitoring and complex event processing (CEP) in IoT systems. EDA could be combined with business process execution languages in order to trigger specific steps or parts of a business process.

2.7.2 Processes Dealing with Unreliable Data

When dealing with events coming from the physical world (e.g., via sensors or signal processing algorithms), a degree of unreliability and uncertainty is introduced into the processes. If decisions in a business process are to be taken based on events that have some uncertainty attached, it makes sense to associate each of these events with some value for the quality of information (QoI). In simple cases, this allows the process modeller to define thresholds: e.g., if the degree of certainty is more than 90%, then it is assumed that the event really happened. If it is between 50% and 90%, some other activities will be triggered to determine if the event occurred or not. If it is below 50%, the event is ignored. Things get more complex when multiple events are involved: e.g., one event with 95% certainty, one with 73%, and another with 52%. The underlying services that fire the original events have to be programmed to attach such QoI values to the events. From a BPM perspective, it is essential that such information can be captured, processed and expressed in the modelling notation language, e.g. BPMN. Secondly, the syntax and semantics of such QoI values need to be standardized. Is it a simple certainty percentage as in the examples above, or should it be something more expressive (e.g., a range within which the true value lies)? Relevant techniques should not only address uncertainty in the flow of a given (well-known) IoT-based

business process, but also in the overall structuring and modelling of (possibly unknown or unstructured) process flows. Techniques for fuzzy modelling of data and processes could be considered.

2.7.3 Processes Dealing with Unreliable Resources

Not only is the data from resources inherently unreliable, but also the resources providing the data themselves, e.g., due to the failure of the hosting device. Processes relying on such resources need to be able to adapt to such situations. The first issue is to detect such a failure. In the case that a process is calling a resource directly, this detection is trivial. When we're talking about resources that might generate an event at one point in time (e.g., the resource that monitors the temperature condition within the truck and sends an alert if it has become too hot), it is more difficult. Not having received any event can be because of resource failure, but also because there was nothing to report. Likewise, the quality of the generated reports should be regularly audited for correctness. Some monitoring software is needed to detect such problems; it is unclear though if such software should be part of the BPM execution environment or should be a separate component. Among the research challenges is the synchronization of monitoring processes with run-time actuating processes, given that management planes (e.g., monitoring software) tend to operate at different time scales from IoT processes (e.g., automation and control systems in manufacturing).

2.7.4 Highly Distributed Processes

When interaction with real-world objects and devices is required, it can make sense to execute a process in a decentralized fashion. As stated in [107], the decomposition and decentralization of existing business processes increases scalability and performance, allows better decision making and could even lead to new business models and revenue streams through entitlement management of software products deployed on smart items. For example, in environmental monitoring or supply chain tracking applications, no messages need to be sent to the central system as long as everything is within the defined limits. Only if there is a deviation, an alert (event) needs to be generated, which in turn can lead to an adaptation of the overall process. From a business process modelling perspective though, it should be possible to define the process

centrally, including the fact that some activities (i.e., the monitoring) will be done remotely. Once the complete process is modelled, it should then be possible to deploy the related services to where they have to be executed, and then run and monitor the complete process.

Relevant research issues include tools and techniques for the synthesis, the verification and the adaptation of distributed processes, in the scope of a volatile environment (i.e. changing contexts, mobility, internet connected objects/devices that join or leave).

2.8 Data Management

Data management is a crucial aspect in the Internet of Things. When considering a world of objects interconnected and constantly exchanging all types of information, the volume of the generated data and the processes involved in the handling of those data become critical.

A long-term opportunity for wireless communications chip makers is the rise of Machine-to-Machine (M2M) computing, which one of the enabling technologies for Internet of Things. This technology spans abroad range of applications. While there is consensus that M2M is a promising pocket of growth, analyst estimates on the size of the opportunity diverge by a factor of four [16]. Conservative estimates assume roughly 80 million to 90 million M2M units will be sold in 2014, whereas more optimistic projections forecast sales of 300 million units. Based on historical analyses of adoption curves for similar disruptive technologies, such as portable MP3 players and antilock braking systems for cars, it is believed that unit sales in M2M could rise by as much as a factor of ten over the next five years, see Figure 2.29 [16].

There are many technologies and factors involved in the "data management" within the IoT context.

Some of the most relevant concepts which enable us to understand the challenges and opportunities of data management are:

- Data Collection and Analysis
- Big Data
- Semantic Sensor Networking
- Virtual Sensors
- Complex Event Processing.

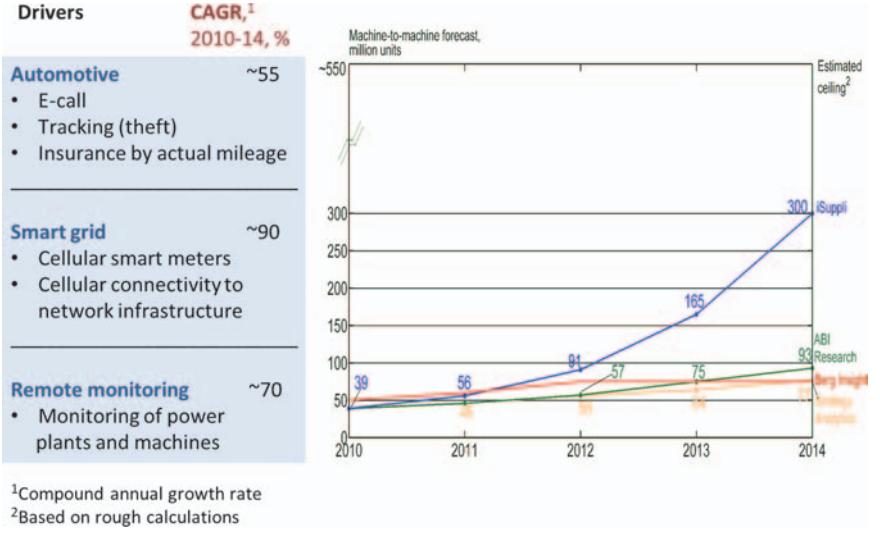

Fig. 2.29 Growth in M2M communications.
(*Source*: ABI research; berg insight; strategy analytics; McKinsey analysis [16]).

2.8.1 Data Collection and Analysis (DCA)

Data Collection and Analysis modules or capabilities are the essential components of any IoT platform or system, and they are constantly evolving in order to support more features and provide more capacity to external components (either higher layer applications leveraging on the data stored by the DCA module or other external systems exchanging information for analysis or processing).

The DCA module is part of the core layer of any IoT platform. Some of the main functions of a DCA module are:

User/customer data storing:

Provides storage of the customer's information collected by sensors

User data & operation modelling:

Allows the customer to create new sensor data models to accommodate collected information and the modelling of the supported operations

On demand data access:

Provides APIs to access the collected data

Device event publish/subscribe/forwarding/notification:

Provides APIs to access the collected data in real time conditions

Customer rules/filtering:

Allows the customer to establish its own filters and rules to correlate events

Customer task automation:

Provides the customer with the ability to manage his automatic processes. Example: scheduled platform originated data collection, …

Customer workflows:

Allows the customer to create his own workflow to process the incoming events from a device

Multitenant structure:

Provides the structure to support multiple organizations and reseller schemes.

In the coming years, the main research efforts should be targeted to some features that should be included in any Data Collection and Analysis platform:

- **Multi-protocol**. DCA platforms should be capable of handling or understanding different input (and output) protocols and formats. Different standards and wrappings for the submission of observations should be supported.
- **De-centralisation**. Sensors and measurements/observations captured by them should be stored in systems that can be de-centralised from a single platform. It is essential that different components, geographically distributed in different locations may cooperate and exchange data. Related with this concept, **federation** among different systems will make possible the global integration of IoT architectures.
- **Security**. DCA platforms should increase the level of data protection and security, from the transmission of messages from devices (sensors, actuators, etc.) to the data stored in the platform.
- **Data mining features**. Ideally, DCA systems should also integrate capacities for the processing of the stored info, making it easier to extract useful data from the huge amount of contents that may be recorded.

2.8.2 Big Data

Big data is about the processing and analysis of large data repositories, so disproportionately large that it is impossible to treat them with the conventional tools of analytical databases. Some statements suggest that we are entering the "Industrial Revolution of Data," [108], where the majority of data will be stamped out by machines. These machines generate data a lot faster than people can, and their production rates will grow exponentially with Moore's Law. Storing this data is cheap, and it can be mined for valuable information. Examples of this tendency include:

- Web logs;
- RFID;
- Sensor networks;
- Social networks;
- Social data (due to the Social data revolution);
- Internet text and documents;
- Internet search indexing;
- Call detail records;
- Astronomy, atmospheric science, genomics, biogeochemical, biological, and other complex and/or interdisciplinary scientific research;
- Military surveillance;
- Medical records;
- Photography archives;
- Video archives;
- Large scale e-commerce.

The trend is part of an environment quite popular lately: the proliferation of web pages, image and video applications, social networks, mobile devices, apps, sensors, and so on, able to generate, according to IBM, more than 2.5 quintillion bytes per day, to the extent that 90% of the world's data have been created over the past two years.

Big data requires exceptional technologies to efficiently process large quantities of data within a tolerable amount of time. Technologies being applied to big data include massively parallel processing (MPP) databases, data-mining grids, distributed file systems, distributed databases, cloud

computing platforms, the Internet, and scalable storage systems. These technologies are linked with many aspects derived from the analysis of natural phenomena such as climate and seismic data to environments such as health, safety or, of course, the business environment.

The biggest challenge of the Petabyte Age will not be storing all that data, it will be figuring out how to make sense of it. Big data deals with unconventional, unstructured databases, which can reach petabytes, exabytes or zettabytes, and require specific treatments for their needs, either in terms of storage or processing/display.

Companies focused on the big data topic, such as Google, Yahoo!, Facebook or some specialised start-ups, currently do not use Oracle tools to process their big data repositories, and they opt instead for an approach based on distributed, cloud and open source systems. An extremely popular example is Hadoop, an Open Source framework in this field that allows applications to work with huge repositories of data and thousands of nodes. These have been inspired by Google tools such as the MapReduce and Google File system, or NoSQL systems, which in many cases do not comply with the ACID (atomicity, consistency, isolation, durability) characteristics of conventional databases.

In future, it is expected a huge increase in adoption, and many, many questions that must be addressed. Among the imminent research targets in this field are:

- **Privacy**. Big data systems must avoid any suggestion that users and citizens in general perceive that their privacy is being invaded.
- Integration of both relational and NoSQL systems.
- More efficient indexing, search and processing algorithms, allowing the extraction of results in reduced time and, ideally, near to "real time" scenarios.
- **Optimised storage of data**. Given the amount of information that the new IoT world may generate, it is essential to avoid that the storage requirements and costs increase exponentially.

2.8.3 Semantic Sensor Networks and Semantic Annotation of Data

The information collected from the physical world in combination with the existing resources and services on the Web facilitate enhanced methods

to obtain business intelligence, enabling the construction of new types of front-end application and services which could revolutionise the way organisations and people use Internet services and applications in their daily activities. Annotating and interpreting the data, and also the network resources, enables management of the large scale distributed networks that are often resource and energy constrained, and provides means that allow software agents and intelligent mechanisms to process and reason the acquired data.

There are currently on-going efforts to define ontologies and to create frameworks to apply semantic Web technologies to sensor networks. The Semantic Sensor Web (SSW) proposes annotating sensor data with spatial, temporal, and thematic semantic metadata [110]. This approach uses the current OGC and SWE [112] specifications and attempts to extend them with semantic web technologies to provide enhanced descriptions to facilitate access to sensor data. W3C Semantic Sensor Networks Incubator Group [113] is also working on developing ontology for describing sensors. Effective description of sensor, observation and measurement data and utilising semantic Web technologies for this purpose, are fundamental steps to the construction of semantic sensor networks.

However, associating this data to the existing concepts on the Web and reasoning the data is also an important task to make this information widely available for different applications, front-end services and data consumers.

Semantics allow machines to interpret links and relations between different attributes of a sensor description and also other resources. Utilising and reasoning this information enables the integration of the data as networked knowledge [115]. On a large scale this machine interpretable information (i.e., semantics) is a key enabler and necessity for the semantic sensor networks. Emergence of sensor data as linked-data enables sensor network providers and data consumers to connect sensor descriptions to potentially endless data existing on the Web. By relating sensor data attributes such as location, type, observation and measurement features to other resources on the Web of data, users will be able to integrate physical world data and the logical world data to draw conclusions, create business intelligence, enable smart environments, and support automated decision making systems among many other applications.

The linked-sensor-data can also be queried, accessed and reasoned based on the same principles that apply to linked-data. The principles of using linked data to describe sensor network resources and data in an implementation of an

open platform to publish and consume interoperable sensor data is described in [116].

In general, associating sensor and sensor network data with other concepts (on the Web) and reasoning makes the data information widely available for different applications, front-end services and data consumers. The semantic description allow machines to interpret links and relations between the different attributes of a sensor description and also other data existing on the Web or provided by other applications and resources. Utilising and reasoning this information enables the integration of the data on a wider scale, known as networked knowledge [115]. This machine-interpretable information (i.e. semantics) is a key enabler for the semantic sensor networks.

2.8.4 Virtual Sensors

A virtual sensor can be considered as a product of spatial, temporal and/or thematic transformation of raw or other virtual sensor producing data with necessary provenance information attached to this transformation. Virtual sensors and actuators are a programming abstraction simplifying the development of decentralized WSN applications [117].

The data acquired by a set of sensors can be collected, processed according to an application-provided aggregation function, and then perceived as the reading of a single virtual sensor. Dually, a virtual actuator provides a single entry point for distributing commands to a set of real actuator nodes. The flow of information between real devices and virtual sensors or actuators is presented in Figure 2.30. We follow that statement with this definition:

- A virtual sensor behaves just like a real sensor, emitting time-series data from a specified geographic region with newly defined thematic concepts or observations which the real sensors may not have.
- A virtual sensor may not have any real sensor's physical properties such as manufacturer or battery power information, but does have other properties, such as: who created it; what methods are used, and what original sensors it is based on.

The virtualization of sensors can be considered at different levels as presented in Figure 2.31. At the lowest level are those related with the more local

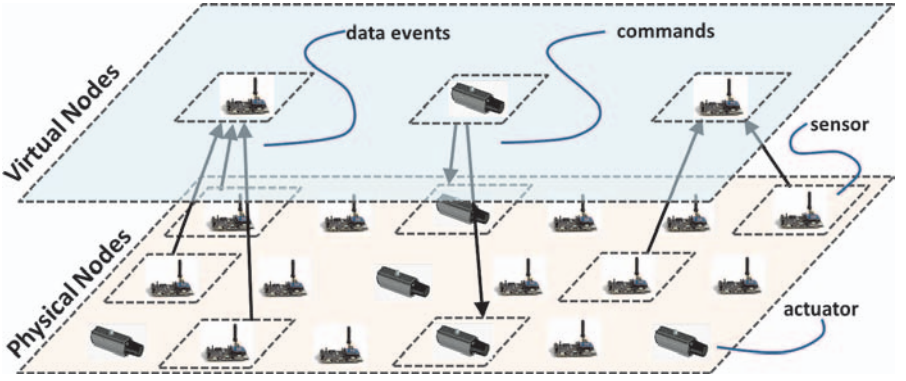

Fig. 2.30 Flow of information between real devices and virtual sensors or actuators [117].

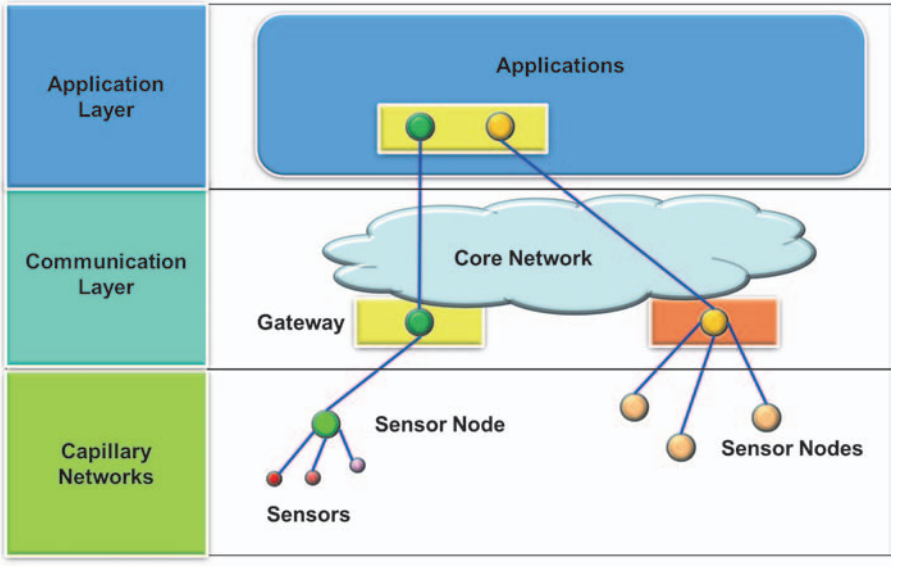

Fig. 2.31 Different levels for sensor virtualization.

processing of several simple measurements (for example in a sensing node), and at the highest level, the abstract combination of different sensors at the application level (including user-generated virtual sensors).

In that sense the development of virtual sensors could be approached following two different degrees of complexity:

- The combination of a limited number of related sensors or measurements to derive new virtual data (usually done at the sensor node or gateway level).
- The complex process of deriving virtual information from a huge space of sensed data (generally at the application level).

Furthermore it is also important to consider that due to the temporal dimension of sensor data most of the processing required to develop virtual sensors is tightly related to the event concept as defined in ISO 19136 “an action that occurs at an instant or over an interval of time", as well as to Event Processing as “creating, deleting, reading and editing of as well as reacting to events and their representations” [118].

An event, as a message indicating that something of interest happens, is usually specified through an event type as a structure of attribute-value tuples. An important attribute is the event occurrence time or its valid time interval. Timing is generally described using timestamps but its proper management presents important challenges in geographically dispersed distributed systems.

The complexity of deriving virtual information from a large number of sensor data as depicted in Figure 2.32, demands the use of proper methods, techniques and tools for processing events while they occur, i.e., in a continuous and timely fashion. Deriving valuable higher-level knowledge from lower-level events has been approached using different technologies from many independent research fields (such as, discrete event simulation,

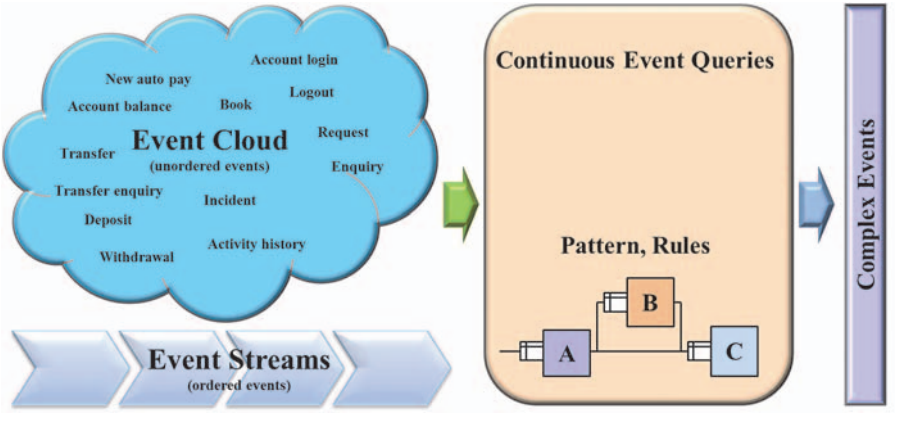

Fig. 2.32 Complex event processing (CEP) and event stream processing (ESP).

active databases, network management, or temporal reasoning), and in different application fields (as business activity monitoring, market data analysis, sensor networks, etc.). Only in recent years has the term Complex Event Processing, CEP, emerged as a discipline of its own and as an important trend in industry applications where it is necessary to detect situations (specified as complex events) that result from a number of correlated (simple) events. CEP concept will be described in depth hereafter.

More specifically, as represented in Figure 2.32, considering that sensor data is generally delivered as a stream, a sub-form of CEP known as Event Stream Processing (ESP) [119] can be used for searching different patterns in continuous streams of sensor data events.

In the near future, some of the main challenges to be solved in the context of Virtual Sensors are:

- **Seamless integration and interoperability of "real" and "virtual" sensors.** This means that virtual sensors should be indistinguishable from real ones for the external or high level applications, but also for other sensors or system modules if necessary. This way, virtual sensors could be fed as input sensors for new virtual ones, making the flexibility and power of this approach almost unlimited.
- **Support of (input) sensors and measurements heterogeneity**. A virtual sensor should, ideally, be capable of handling input sensors of a very different nature. This results in a very powerful mechanism for implementing complex logics, also linking with CEP concepts. The integration of sensors capturing different phenomena may help the implementation of heuristics or artificial intelligence-based decision modules, capable of handling aspects that are not homogeneous (not mere statistics functions over homogeneous figures). This also includes the automatic handling or conversion of different units or scales for input sensors measuring a same aspect.
- Definition of virtual sensors based on **semantic rules**. A first approach for defining virtual sensors is by implementing the programmatic logic or processes associated with the "operation" to be performed by the sensor. But a much richer and more powerful scheme can be obtained if sensors can be defined by "high level" semantic rules (only describing the general behaviour or

expected results) and implementation steps are automatically generated (from the rules) or hidden to external users.

2.8.5 Complex Event Processing

A concept linked with the notion and appearance of "Virtual Sensors" is the Complex Event Processing, in the sense that Virtual Sensors can be used to implement "single sensors" from complex and multiple (actual) sensors or various data sources, thus providing a seamless integration and processing of complex events in a sensor (or Data Collection and Analysis) platform or system.

Complex event processing (CEP) is an emerging network technology that creates actionable, situational knowledge from distributed message-based systems, databases and applications in real time or near real time. CEP can provide an organization with the capability to define, manage and predict events, situations, exceptional conditions, opportunities and threats in complex, heterogeneous networks. Many have said that advancements in CEP will help advance the state-of-the-art in end-to-end visibility for operational situational awareness in many business scenarios (*The CEP Blog*) [120]. These scenarios range from network management to business optimization, resulting in enhanced situational knowledge, increased business agility, and the ability to more accurately (and rapidly) sense, detect and respond to business events and situations.

CEP is a technology for extracting higher level knowledge from situational information abstracted from processing sensory information and for low-latency filtering, correlating, aggregating, and computing on real-world event data. It is an emerging network technology that creates actionable, situational knowledge from distributed message-based systems, databases and applications in real-time or near real-time.

2.8.5.1 Types

Most CEP solutions and concepts can be classified into two main categories:

- **Computation-oriented CEP:** Focused on executing on-line algorithms as a response to event data entering the system. A simple example is to continuously calculate an average based on data from the inbound events

- **Detection-oriented CEP:** Focused on detecting combinations of events called event patterns or situations. A simple example of detecting a situation is to look for a specific sequence of events.

Some of the research topics for the immediate future in the context of CEP are:

- **Distributed CEP:** Since CEP core engines usually require powerful hardware and complex input data to consider, it is not easy to design and implement distributed systems capable of taking consistent decisions from non-centralised resources.
- **Definition of standardised interfaces:** Currently, most of the CEP solutions are totally proprietary and not compliant with any type of standard format or interface. In addition, it is not easy to integrate these processes in other systems in an automated way. It is essential to standardise input and output interfaces in order to make CEP systems interoperable among themselves (thus enabling exchanging of input events and results) and to ease integration of CEP in other systems, just as any other step in the transformation or processing of data.
- **Improved security and privacy policies:** CEP systems often imply the handling of "private" data that are incorporated to decision taking or elaboration of more complex data. It is necessary that all processes and synthetic data can be limited by well-defined rules and security constraints (that must be measurable, traceable and verifiable).

2.9 Security, Privacy & Trust

The Internet of Things presents security-related challenges that are identified in the IERC 2010 Strategic Research and Innovation Roadmap but some elaboration is useful as there are further aspects that need to be addressed by the research community. While there are a number of specific security, privacy and trust challenges in the IoT, they all share a number of transverse non-functional requirements:

- Lightweight and symmetric solutions, Support for resource constrained devices
- Scalable to billions of devices/transactions

Solutions will need to address federation/administrative co-operation

- Heterogeneity and multiplicity of devices and platforms
- Intuitively usable solutions, seamlessly integrated into the real world

2.9.1 Trust for IoT

As IoT-scale applications and services will scale over multiple administrative domains and involve multiple ownership regimes, there is a need for a trust framework to enable the users of the system to have confidence that the information and services being exchanged can indeed be relied upon. The trust framework needs to be able to deal with humans and machines as users, i.e. it needs to convey trust to humans and needs to be robust enough to be used by machines without denial of service. The development of trust frameworks that address this requirement will require advances in areas such as:

- Lightweight Public Key Infrastructures (PKI) as a basis for trust management. Advances are expected in hierarchical and cross certification concepts to enable solutions to address the scalability requirements.
- Lightweight key management systems to enable trust relationships to be established and the distribution of encryption materials using minimum communications and processing resources, as is consistent with the resource constrained nature of many IoT devices.
- Quality of Information is a requirement for many IoT-based systems where metadata can be used to provide an assessment of the reliability of IoT data.
- Decentralised and self-configuring systems as alternatives to PKI for establishing trust e.g. identity federation, peer to peer.
- Novel methods for assessing trust in people, devices and data, beyond reputation systems. One example is Trust Negotiation. Trust Negotiation is a mechanism that allows two parties to automatically negotiate, on the basis of a chain of trust policies, the minimum level of trust required to grant access to a service or to a piece of information.
- Assurance methods for trusted platforms including hardware, software, protocols, etc.

- Access Control to prevent data breaches. One example is Usage Control, which is the process of ensuring the correct usage of certain information according to a predefined policy after the access to information is granted.

2.9.2 Security for IoT

As the IoT becomes a key element of the Future Internet and a critical national/international infrastructure, the need to provide adequate security for the IoT infrastructure becomes ever more important. Large-scale applications and services based on the IoT are increasingly vulnerable to disruption from attack or information theft. Advances are required in several areas to make the IoT secure from those with malicious intent, including.

- DoS/DDOS attacks are already well understood for the current Internet, but the IoT is also susceptible to such attacks and will require specific techniques and mechanisms to ensure that transport, energy, city infrastructures cannot be disabled or subverted.
- General attack detection and recovery/resilience to cope with IoT-specific threats, such as compromised nodes, malicious code hacking attacks.
- Cyber situation awareness tools/techniques will need to be developed to enable IoT-based infrastructures to be monitored. Advances are required to enable operators to adapt the protection of the IoT during the lifecycle of the system and assist operators to take the most appropriate protective action during attacks.
- The IoT requires a variety of access control and associated accounting schemes to support the various authorisation and usage models that are required by users. The heterogeneity and diversity of the devices/gateways that require access control will require new lightweight schemes to be developed.
- The IoT needs to handle virtually all modes of operation by itself without relying on human control. New techniques and approaches e.g. from machine learning, are required to lead to a self-managed IoT.

2.9.3 Privacy for IoT

As much of the information in an IoT system may be personal data, there is a requirement to support anonymity and restrictive handling of personal information.

There are a number of areas where advances are required:

- Cryptographic techniques that enable protected data to be stored processed and shared, without the information content being accessible to other parties. Technologies such as homomorphic and searchable encryption are potential candidates for developing such approaches.
- Techniques to support Privacy by Design concepts, including data minimisation, identification, authentication and anonymity.
- Fine-grain and self-configuring access control mechanism emulating the real world.

There are a number of privacy implications arising from the ubiquity and pervasiveness of IoT devices where further research is required, including:

- Preserving location privacy, where location can be inferred from things associated with people.
- Prevention of personal information inference, that individuals would wish to keep private, through the observation of IoT-related exchanges.
- Keeping information as local as possible using decentralised computing and key management.
- Use of soft identities, where the real identity of the user can be used to generate various soft identities for specific applications. Each soft identity can be designed for a specific context or application without revealing unnecessary information, which can lead to privacy breaches.

2.10 Device Level Energy Issues

One of the essential challenges in IoT is how to interconnect "things" in an interoperable way while taking into account the energy constraints, knowing that the communication is the most energy consuming task on devices. RF

solutions for a wide field of applications in the Internet of Things have been released over the last decade, led by a need for integration and low power consumption.

2.10.1 Low Power Communication

Several low power communication technologies have been proposed from different standardisation bodies. The most common ones are:

- **IEEE 802.15.4** has developed a low-cost, low-power consumption, low complexity, low to medium range communication standard at the link and the physical layers [122] for resource constrained devices.
- **Bluetooth low energy** (Bluetooth LE, [123]) is the ultra-low power version of the Bluetooth technology [124] that is up to 15 times more efficient than Bluetooth.
- **Ultra-Wide Bandwidth (UWB) Technology** [125] is an emerging technology in the IoT domain that transmits signals across a much larger frequency range than conventional systems. UWB, in addition to its communication capabilities, it can allow for high precision ranging of devices in IoT applications.
- **RFID/NFC** proposes a variety of standards to offer contact less solutions. Proximity cards can only be read from less than 10 cm and follows the ISO 14443 standard [126] and is also the basis of the NFC standard. RFID tags or vicinity tags dedicated to identification of objects have a reading distance which can reach 7 to 8 meters.

Nevertheless, front-end architectures have remained traditional and there is now a demand for innovation. Regarding the ultra-low consumption target, super-regenerative have proven to be very energetically efficient architectures used for Wake-Up receivers. It remains active permanently at very low power consumption, and can trigger a signal to wake up a complete/standard receiver [127, 128]. In this field, standardisation is required, as today only proprietary solutions exist, for an actual gain in the overall market to be significant.

On the other hand, power consumption reduction of an RF full-receiver can be envisioned, with a target well below 5 mW to enable very small form

factor and long life-time battery. Indeed, targeting below 1 mW would then enable support from energy harvesting systems enabling energy autonomous RF communications. In addition to this improvement, lighter communication protocols should also be envisioned as the frequent synchronization requirement makes frequent activation of the RF link mandatory, thereby overhead in the power consumption.

It must also be considered that recent advances in the area of CMOS technology beyond 90 nm, even 65 nm nodes, leads to new paradigms in the field of RF communication. Applications which require RF connectivity are growing as fast as the Internet of Things, and it is now economically viable to propose this connectivity solution as a feature of a wider solution. It is already the case for the micro-controller which can now easily embed a ZigBee or Bluetooth RF link, and this will expand to meet other large volume applications sensors.

Progressively, portable RF architectures are making it easy to add the RF feature to existing devices. This will lead to RF heavily exploiting digital blocks and limiting analogue ones, like passive/inductor silicon consuming elements, as these are rarely easy to port from one technology to another. Nevertheless, the same performance will be required so receiver architectures will have to efficiently digitalize the signal in the receiver or transmitter chain [129]. In this direction, Band-Pass Sampling solutions are promising as the signal is quantized at a much lower frequency than the Nyquist one, related to deep under-sampling ratio [130]. Consumption is therefore greatly reduced compared to more traditional early-stage sampling processes, where the sampling frequency is much lower.

Continuous-Time quantization has also been regarded as a solution for high-integration and easy portability. It is an early-stage quantization as well, but without sampling [131]. Therefore, there is no added consumption due to the clock, only a signal level which is considered. These two solutions are clear evolutions to pave the way to further digital and portable RF solutions.

Cable-powered devices are not expected to be a viable option for IoT devices as they are difficult and costly to deploy. Battery replacements in devices are either impractical or very costly in many IoT deployment scenarios. As a consequence, for large scale and autonomous IoT, alternative energy sourcing using ambient energy should be considered.

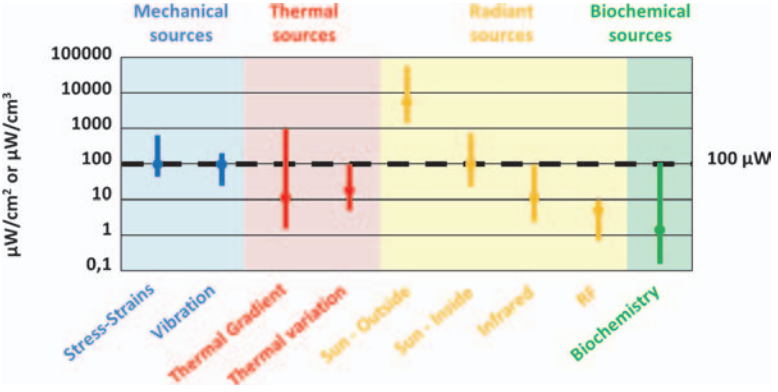

Fig. 2.33 Ambient sources' power densities before conversion. (*Source*: CEA-Leti).

2.10.2 Energy Harvesting

Four main ambient energy sources are present in our environment: mechanical energy, thermal energy, radiant energy and chemical energy. These sources are characterized by different power densities (Figure 2.33).

Energy harvesting (EH) must be chosen according to the local environment. For outside or luminous indoor environments, solar energy harvesting is the most appropriate solution. In a closed environment thermal or mechanical energy may be a better alternative. It is mainly the primary energy source power density in the considered environment that defines the electrical output power that can be harvested and not the transducer itself. The figure also shows that, excluding "sun-outside", 10–100 μW is a fair order of magnitude for 1 cm^2 or 1 cm^3-EH output power [132].

Low power devices are expected to require 50 mW in transmission mode and less in standby or sleep modes. EH devices cannot supply this amount of energy in a continuous active mode, but instead intermittent operation mode can be used in EH-powered devices.

The sensor node's average power consumption corresponds to the total amount of energy needed for one measurement cycle multiplied by the frequency of the operation.

For example, harvesting 100 μW during 1 year corresponds to a total amount of energy equivalent to 1 g of lithium.

Considering this approach of looking at energy consumption for one measurement instead of average power consumption, it results that, today:

- Sending 100 bits of data consumes about 5 μJ,
- Measuring acceleration consumes about 50 μJ,
- Making a complete measurement: measure + conversion + emission consume 250–500 μJ.

Therefore, with 100 μW harvested continuously, it is possible to perform a complete measurement every 1–10 seconds. This duty cycle can be sufficient for many applications. For other applications, basic functions' power consumptions are expected to be reduced by 10 to 100 within 10 years; which will enable continuous running mode of EH-powered IoT devices.

Even though many developments have been performed over the last 10 years, energy harvesting — except PV cells — is still an emerging technology that has not yet been adopted by industry. Nevertheless, further improvements of present technologies should enable the needs of IoT to be met.

An example of interoperable wireless standard that enables switches, gateways and sensors from different manufacturers to combine seamlessly and wireless communicates with all major wired bus systems such as KNX, LON, BACnet or TCP/IP is presented in [120].

The energy harvesting wireless sensor solution is able to generate a signal from an extremely small amount of energy. From just 50 μWs a standard energy harvesting wireless module can easily transmit a signal 300 meters (in a free field).

2.10.3 Future Trends and Recommendations

In the future, the number and types of IoT devices will increase, therefore inter-operability between devices will be essential. More computation and yet less power and lower cost requirements will have to be met. Technology integration will be an enabler along with the development of even lower power technology and improvement of battery efficiency. The power consumption of computers over the last 60 years was analysed in [133] and the authors concluded that electrical efficiency of computation has doubled roughly every year and a half. A similar trend can be expected for embedded computing using similar technology over the next 10 years. This would lead to a reduction by

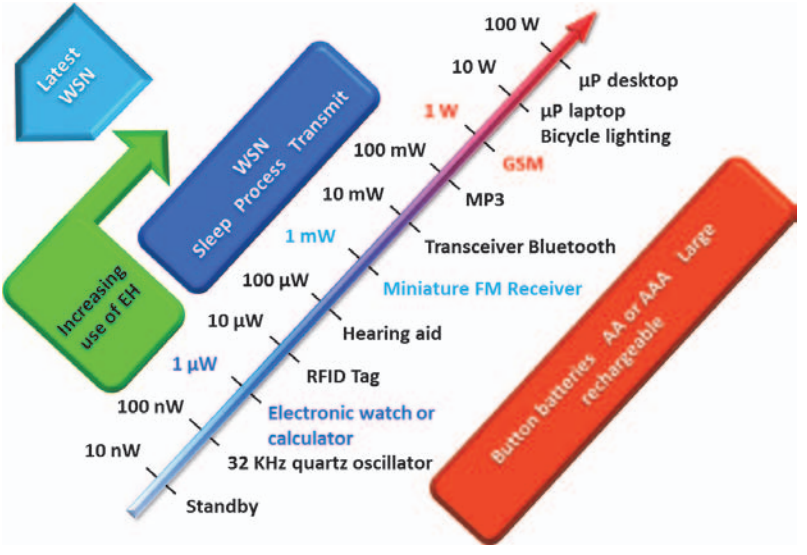

Fig. 2.34 Power consumption requirements for different devices.

an order of 100 in power consumption at same level of computation. Allowing for a 10 fold increase in IoT computation, power consumption should still be reduced by an order of 10. An example of power consumption requirements for different devices is given in Figure 2.34.

On the other hand, energy harvesting techniques have been explored to respond to the energy consumption requirements of the IoT domain. For vibration energy harvesters, we expect them to have higher power densities in the future (from 10 μW/g to 30 μW/g) and to work on a wider frequency bandwidth. A roadmap of vibration energy harvesters is provided in Figure 2.36.

Actually, the goal of vibration energy harvesters' researchers is to develop Plug and Play (PnP) devices, able to work in any vibrating environment, within 10 years. In the same time, we expect basic functions' energy consumption to decrease by at least a factor of 10. All these progresses will allow vibration energy harvesters to attract new markets, from industry to healthcare or defence.

The main challenge for thermoelectric solutions is to increase thermoelectric materials' intrinsic efficiency, in order to convert a higher part of the few mW of thermal energy available. This efficiency improvement will be

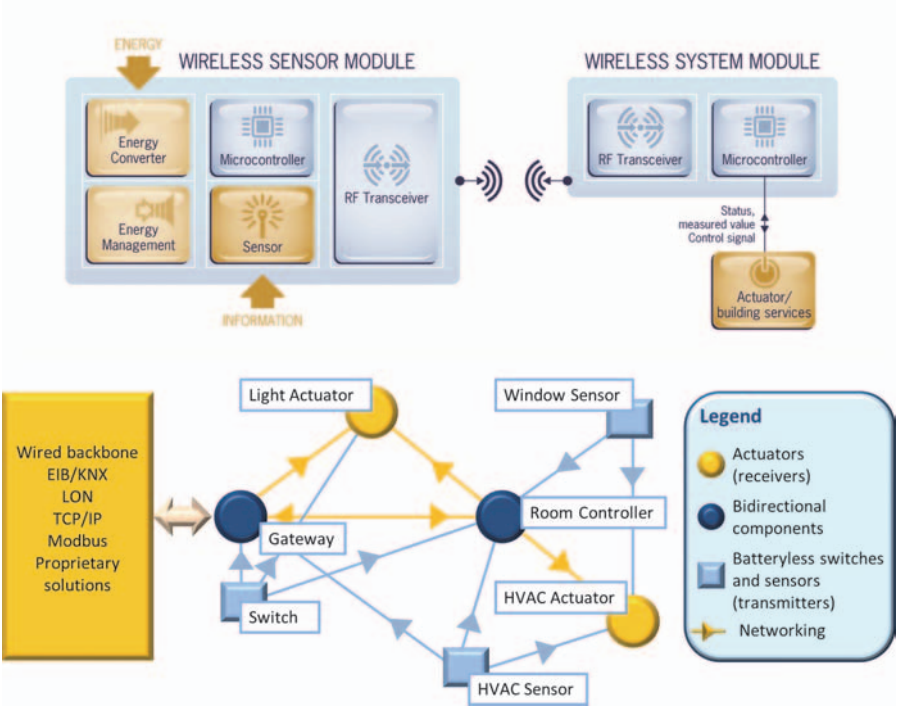

Fig. 2.35 Energy harvesting wireless sensor network. (*Source*: EnOcean).

mainly performed by using micro and nanotechnologies (such as superlattices or quantum dots).

For solar energy harvesting, photovoltaic cells are probably the most advanced and robust solution. They are already used in many applications and for most of them, today's solutions are sufficient. Yet, for IoT devices, it could be interesting to improve the photovoltaic cells efficiency to decrease photovoltaic cells' sizes and to harvest energy in even darker places.

2.11 IoT Related Standardisation

The IERC previous SRAs [19, 29] addresses the topic of standardisation and is focused on the actual needs of producing specific standards. This chapter examines further standardisation considerations.

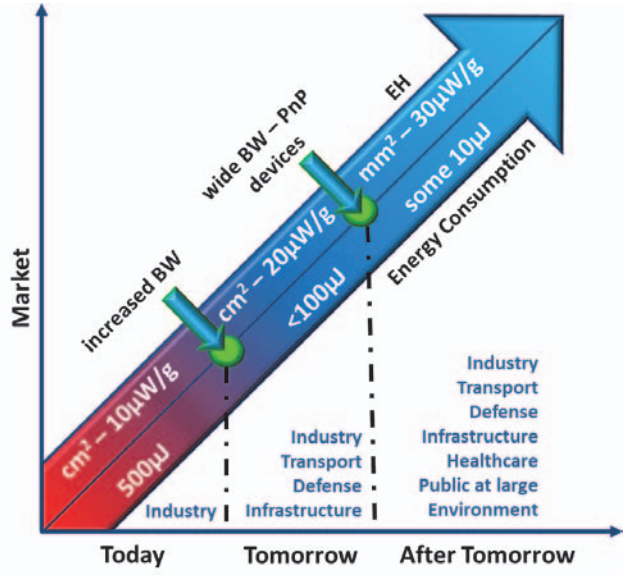

Fig. 2.36 Roadmap for vibration energy harvesters. (*Source*: CEA-Leti).

2.11.1 The Role of Standardisation Activities

Standards are needed for interoperability both within and between domains. Within a domain, standards can provide cost efficient realizations of solutions, and a domain here can mean even a specific organization or enterprise realizing an IoT. Between domains, the interoperability ensures cooperation between the engaged domains, and is more oriented towards Internet of Things applications. There is a need to consider the life-cycle process in which standardisation is one activity. Significant attention is given to the "pre-selection" of standards through collaborative research, but focus should also be given to regulation, legislation, interoperability and certification as other activities in the same life-cycle. For IoT, this is of particular importance.

A complexity with IoT comes from the fact that IoT intends to support a number of different applications covering a wide array of disciplines that are not part of the ICT domain. Requirements in these different disciplines can often come from legislation or regulatory activities. As a result, such policy making can have a direct requirement for supporting IoT standards to be developed. It would therefore be beneficial to develop a wider approach

to standardisation and include anticipation of emerging or on-going policy making in target application areas, and thus be prepared for its potential impact on IoT-related standardisation.

A typical example is the standardisation of vehicle emergency call services called eCall driven from the EC [134]. Based on the objective of increased road safety, directives were established that led to the standardisation of solutions for services and communication by e.g. ETSI, and subsequently 3GPP. Another example is the Smart Grid standardisation mandate M/490 [135] from the EC towards the European Standards Organisations (ESOs), and primarily ETSI, CEN and CENELEC.

The standardisation bodies are addressing the issue of interoperable protocol stacks and open standards for the IoT. This includes as well expending the HTTP, TCP, IP stack to the IoT-specific protocol stack. This is quite challenging considering the different wireless protocols like ZigBee, RFID, Bluetooth, BACnet 802.15.4e, 6LoWPAN, RPL, and CoAP. One difference between HTTP and CoAP is the transport layer. HTTP relies on the Transmission Control Protocol (TCP). TCP's flow control mechanism is not appropriate for LLNs and its overhead is considered too high for short-lived transactions. In addition, TCP does not have multicast support and is rather sensitive to mobility. CoAP is built on top of the User Datagram Protocol (UDP) and therefore has significantly lower overhead and multicast support [45].

The conclusion is that any IoT related standardisation must pay attention to how regulatory measures in a particular applied sector will eventually drive the need for standardized efforts in the IoT domain.

Agreed standards do not necessarily mean that the objective of interoperability is achieved. The mobile communications industry has been successful not only because of its global standards, but also because interoperability can be assured via the certification of mobile devices and organizations such as the Global Certification Forum [136] which is a joint partnership between mobile network operators, mobile handset manufacturers and test equipment manufacturers. Current corresponding M2M efforts are very domain specific and fragmented. The emerging IoT and M2M dependant industries should also benefit from ensuring interoperability of devices via activities such as conformance testing and certification on a broader scale.

To achieve this very important objective of a "certification" or validation programme, we also need non ambiguous test specifications which are

also standards. This represents a critical step and an economic issue as this activity is resource consuming. As for any complex technology, implementation of test specifications into cost-effective test tools should also to be considered. A good example is the complete approach of ETSI using a methodology (e.g. based on TTCN-3) considering all the needs for successful certification programmes.

The conclusion therefore is that just as the applied sector can benefit from standards supporting their particular regulated or mandated needs, equally, these sectors can benefit from conforming and certified solutions, protocols and devices. This is certain to help the IoT-supporting industrial players to succeed.

It is worth noting that setting standards for the purpose of interoperability is not only driven by proper SDOs, but for many industries and applied sectors it can also be driven by Special Interest Groups, Alliances and the Open Source communities. It is of equal importance from an IoT perspective to consider these different organizations when addressing the issue of standardisation.

From the point of view of standardisation IoT is a global concept, and is based on the idea that anything can be connected at any time from any place to any network, by preserving the security, privacy and safety. The concept of connecting any object to the Internet could be one of the biggest standardisation challenges and the success of the IoT is dependent on the development of interoperable global standards. In this context the IERC position is very clear. Global standards are needed to achieve economy of scale and interworking. Wireless sensor networks, RFID, M2M are evolving to intelligent devices which need networking capabilities for a large number of applications and these technologies are "edge" drivers towards the Internet of Things, while the network identifiable devices will have an impact on telecommunications networks. IERC is focussed to identify the requirements and specifications from industry and the needs of IoT standards in different domains and to harmonize the efforts, avoid the duplication of efforts and identify the standardisation areas that need focus in the future.

To achieve these goals it is necessary to overview the international IoT standardisation items and associated roadmap; to propose a harmonized European IoT standardisation roadmap; work to provide a global harmonization of IoT standardisation activities; and develop a basic framework of standards (e.g., concept, terms, definition, relation with similar technologies).

2.11.2 Current Situation

The current M2M related standards and technologies landscape is highly fragmented. The fragmentation can be seen across different applied domains where there is very little or no re-use of technologies beyond basic communications or networking standards. Even within a particular applied sector, a number of competing standards and technologies are used and promoted. The entire ecosystem of solution providers and users would greatly benefit from less fragmentation and should strive towards the use of a common set of basic tools. This would provide faster time to market, economy of scale and reduce overall costs.

Another view is standards targeting protocols vs. systems. Much emphasis has been put on communications and protocol standards, but very little effort has previously been invested in standardizing system functions or system architectures that support IoT. Localized system standards are plentiful for specific deployments in various domains. One such example is in building automation and control with (competing) standards like BACnet and KNX. However, system standards on the larger deployment and global scale are not in place. The on-going work in ETSI M2M TC is one such approach, but is currently limited to providing basic application enablement on top of different networks. It should also be noted that ETSI represent one industry — the telecommunications industry. The IoT stakeholders are represented by a number of different industries and sectors reaching far beyond telecommunications.

2.11.3 Areas for Additional Consideration

The technology fragmentation mentioned above is particularly evident on the IoT device side. To drive further standardisation of device technologies in the direction of standard Internet protocols and Web technologies, and towards the application level, would mitigate the impacts of fragmentation and strive towards true interoperability. Embedded web services, as driven by the IETF and IPSO Alliance, will ensure a seamless integration of IoT devices with the Internet. It will also need to include semantic representation of IoT device hosted services and capabilities.

The service layer infrastructure will require standardisation of necessary capabilities like interfaces to information and sensor data repositories,

discovery and directory services and other mechanisms that have already been identified in projects like SENSEI [137], IoT-A [138], and IoT6. Current efforts in ETSI M2M TC do not address these aspects.

The IoT will require federated environments where producers and consumers of services and information can collaborate across both administrative and application domains. This will require standardized interfaces on discovery capabilities as well as the appropriate semantic annotation to ensure that information becomes interoperable across sectors. Furthermore, mechanisms for authentication and authorization as well as provenance of information, ownership and "market mechanisms" for information become particularly important in a federated environment. Appropriate SLAs will be required for standardisation. F-ONS [141] is one example activity in the direction of federation by GS1. Similar approaches will be needed in general for IoT including standardized cross-domain interfaces of sensor based services.

A number of IoT applications will be coming from the public sector. The Directive on Public Sector Information [142] requires open access to data. Integration of data coming from various application domains is not an easy task as data and information does not adhere to any standardized formats including their semantics. Even within a single domain, data and information is not easily integrated or shared. Consideration of IoT data and information integration and sharing within domains as well as between domains need, also be considered at the international level.

Instrumental in a number of IoT applications is the spatial dimension. Standardisation efforts that provide necessary harmonization and interoperability with spatial information services like INSPIRE [143] will be the key.

IoT with its envisioned billions of devices producing information of very different characteristics will place additional requirements on the underlying communications and networking strata. Efforts are needed to ensure that the networks can accommodate not only the number of devices but also the very different traffic requirements including delay tolerance, latency and reliability. This is of particular importance for wireless access networks which traditionally have been optimized based on a different set of characteristics. 3GPP, as an example, has acknowledged this and has started to address the short term needs, but the long term needs still require identification and standardisation.

2.11.4 Interoperability in the Internet of Things

The Internet of Things is shaping the evolution of the future Internet. After connecting people anytime and everywhere, the next step is to interconnect heterogeneous things/machines/smart objects both between themselves and with the Internet; allowing by thy way, the creation of value-added open and interoperable services/applications, enabled by their interconnection, in such a way that they can be integrated with current and new business and development processes.

As for the IoT, future networks will continue to be heterogeneous, multi-vendors, multi-services and largely distributed. Consequently, the risk of non-interoperability will increase. This may lead to unavailability of some services for end-users that can have catastrophic consequences regarding applications related for instance to emergency or health, etc. Or, it could also mean that users/applications are likely to loose key information out of the IoT due to this lack of interoperability. Thus, it is vital to guarantee that network components will interoperate to unleash the full value of the Internet of Things.

2.11.4.1 IoT interoperability necessary framework

Interoperability is a key challenge in the realms of the Internet of Things. This is due to the intrinsic fabric of the IoT as: (i) *high–dimensional*, with the co-existence of many systems (devices, sensors, equipment, etc.) in the environment that need to communicate and exchange information; (ii) *highly-heterogeneous*, where these vast systems are conceived by a lot of manufacturers and are designed for much different purposes and targeting diverse application domains, making it extremely difficult (if not impossible) to reach out for global agreements and widely accepted specification; (iii) *dynamic and non-linear*, where new Things (that were not even considered at start) are entering (and leaving) the environment all the time and that support new unforeseen formats and protocols but that need to communicate and share data in the IoT; and (iv) *hard to describe/model* due to existence of many data formats, described in much different languages, that can share (or not) the same modelling principles, and that can be interrelated in many ways with one another. **This qualifies interoperability in the IoT as a problem of complex nature!**

Also, the Internet of Things can be seen as both the first and the final frontier of interoperability. First, as it is the initial mile of a sensing system and where interoperability would enable Things to talk and collaborate altogether for an higher purpose; and final, as it is possibly the place where interoperability is more difficult to tackle due to the unavoidable complexities of the IoT. We therefore need some novel approaches and comprehensions of Interoperability for the Internet of Things also making sure that it endures, that it is sustainable. **It is then needed sustainable interoperability in the Internet of Things!**

This means that we need to cope at the same time with the complex nature and sustainability requirement of interoperability in the Internet of Things. For this, it is needed a framework for sustainable interoperability that especially targets the Internet of Things taking on its specifics and constraints. This framework can (and should) learn from the best-of-breed interoperability solutions from related domains (e.g. enterprise interoperability), to take the good approaches and principles of these while understanding the differences and particulars that the Internet of Things poses. The **framework for sustainable interoperability in Internet of Things applications** needs (at least) to address the following aspects:

- *Management of Interoperability in the IoT*: In order to correctly support interoperability in the Internet of Things one needs to efficiently and effectively manage interoperability resources. **What then needs to be managed, to what extent and how, in respect to interoperability in the Internet of Things?**
- Dynamic Interoperability Technologies for the IoT: In order for interoperability to endure in the complex IoT environment, one needs to permit Things to enter and dynamically interoperate without the need of being remanufactured. Then, what approaches and methods to create dynamic interoperability in IoT?
- Measurement of Interoperability in the IoT: In order to properly manage and execute interoperability in the IoT it needs to quantify and/or qualify interoperability itself. As Lord Kelvin stated: "If one can not measure it, one can not improve it". Then, **what methods and techniques to provide an adequate measurement of Interoperability in the Internet of Things?**
- Interaction and integration of IoT in the global Internet: IPv6 integration, global interoperability, IoT-Cloud integration, etc. In

other words, how to bridge billion of smart things globally, while respecting their specific constraints.

2.11.4.2 Technical IoT Interoperability

There are different areas on interoperability such as at least four areas on technical interoperability, syntactic, semantic interoperability and organizational interoperability. **Technical Interoperability** is usually associated with hardware/software components, systems and platforms that enable machine-to-machine communication to take place. This kind of interoperability is often centred on (communication) protocols and the infrastructure needed for those protocols to operate and we need to pay a specific attention as many protocols are developed within SDOs and therefore it will require market proof approach to validate and implement these protocols leading to have true interoperable and global IoT products.

3 pillars of interoperability

Interoperability cannot be ensured properly without unambiguous specification, market accepted unambiguous test specifications and finally some pragmatic evidence of multi-vendors interoperability.

More detail can be found in the ETSI White Paper on Interoperability [144] introducing that in the last few years the nature of using technologies based on stable market–accepted standards has fundamentally shifted. Complex technologies are implemented from 'islands of standards', sometimes coming from many different organisations, sometimes comprising hundreds of different documents.

Resultant products need to fit into this technology standards map both on the *vertical* and the *horizontal* plane. Applications need to interoperate across different domains, as well as directly interworking with underlying layers. This complex ecosystem means that issues of interoperability are more likely to arise and the problem is more critical than ever. The standardisation process is represented in Figure 2.37.

The White Paper documents the need to take care of the consistency of the base "specifications" or standards and on the importance of unambiguous and well accepted test specifications. This part is often underestimated or left alone to the market forces and in such cases lead to large

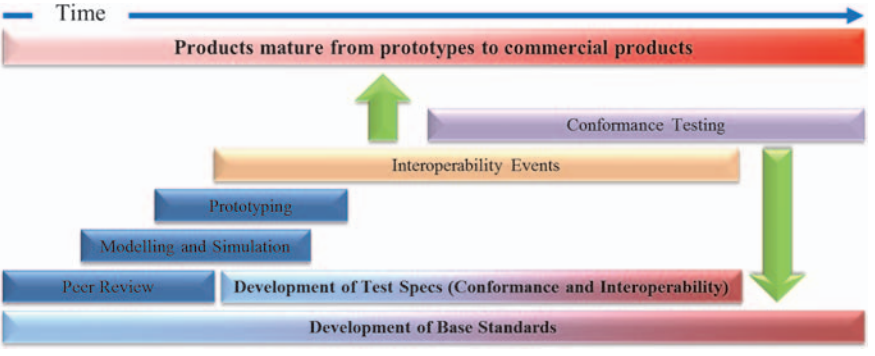

Fig. 2.37 Standardisation process.
(*Source*: ETSI).

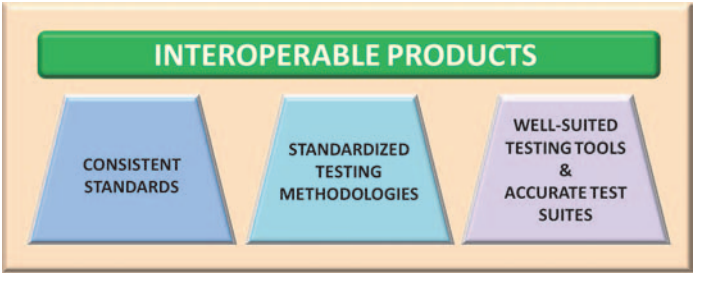

Fig. 2.38 3 pillars to address and improve interoperability.

technologies deployment failures. Although the market forces are pushing for cost-effective developments and these concern huge collective investment on base specifications, test specifications, test tools, validation and certification programmes, the total cost of "doing nothing" is largely more than to think to it start from the beginning. *That requires also research effort in line with the complexity of the research topics*

To sum up, according to experience (e.g. Fora and SDOs approaches to interoperability), we can consider 3 pillars to address and improve interoperability, see Figure 2.38:

- We need **consistent standards** as that is the first and main sources of potential different interpretations and non-interoperable issues
- We need also **test specification and methodologies** to ensure consistent proof of validation or conformity to standards (or industry specifications)

- Even if specifications (base and tests) are available, a final source of non-interoperability and important resources can come for the **test-tools** which will execute the tests and at the end give the final "ok"

All these 3 pillars need to be carefully considered and harmoniously coordinated.

Cost-Time-Quality challenges

Success of worldwide interoperable mobile (GSM) products was also achieved thanks to well defined and detailed tests, tools and certification program as still today run by the GCF (GSM Certification Forum). However the amount of investment done in these matters by in this case and the cost associated per product cannot be repeated for a mass and cheap IoT market. Any cost associated to interoperability should be low and therefore the full chain of activities leading to reasonable level of interoperability need to be optimized.

Any efforts and associated research in optimizing the full chain approach should help to ensure high level of quality and final interoperability while optimizing resources associated to the necessary development of test specifications and tools. To achieve that, also taken into account, the broad range of protocols and aspects covered by an IoT we need to develop automated approach and use state-of-the-art validation methodologies such as, mention only one, the MBT (Model Based Testing) approach which is more and more supported by the market.

The Figure 2.39 represents the various important steps and areas which influence interoperability as well as the areas where challenges exist on term of resources.

To conclude, for Interoperability program(s) on IoT products to succeed, it would be needed to use standardized and advanced test methodologies allowing to addressing the full chain of interoperability as well as to optimize resources while ensuring high level of quality.

Validation

Validation is an important aspect of interoperability (also in the Internet of Things). Testing and Validation provide the assurance that interoperability methods, protocols, etc. can cope with the specific nature and requirements of the Internet of Things.

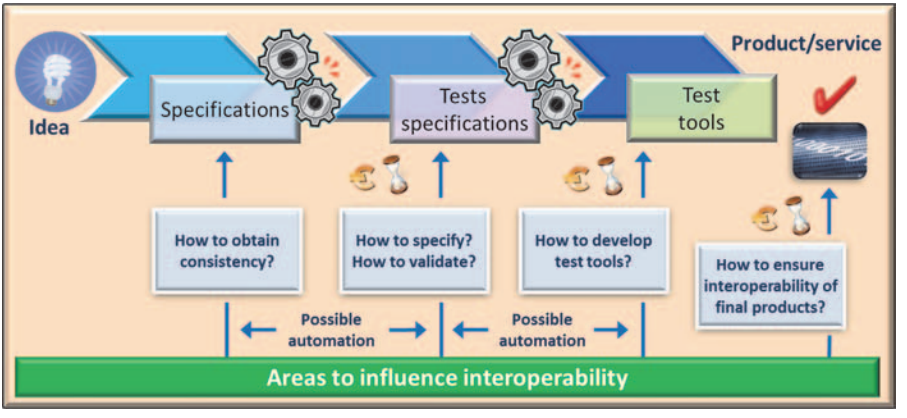

Fig. 2.39 Areas influencing interoperability.

The main way, among others, is to provide **efficient and accurate test suites and associated interoperability testing methodology** (with associated test description/coding languages) that help in testing thoroughly both the underlying protocols used by interconnected things/machines/smart objects and the embedded services/applications. The testing features and facilities need to become build into the design and deployment process, as the conditions of communication means, object/things availability and accessibility may change over time or location.

It is really important that these new testing methods consider the real context of future communicating systems where these objects will be deployed. Indeed, contrary to most of the existing testing methods, interconnected things/machines/smart objects in the IoT are naturally distributed. As they are distributed, the usual and classical approach of a single centralized testing system dealing with all these components and the test execution is no more applicable. The distributed nature of the tested components imposes to move towards distributed testing methods. To be more confident in the real interoperability of these components when they will be deployed in real networks, testing has to be done in a (close to) real operational environment. In Internet of Things applications objects are connected through radio links where the communicating environment may be unreliable and non-controllable. In this context the interoperability testing challenges have to be addressed from the specifications and requirements phase. **Research in IoT challenges leads to IoT validation and interoperability challenges**.

2.12 Recommendations on Research Topics

2.12.1 Applications

Applications of IoT are numerous, permeating into almost all domains of everyday life and activities of individuals and organizations. The challenges are numerous, varied and often related to a particular domain or the context in which an application is used. Abstracting those context specific challenges, the following are considered to be crucial for the successful development and adoption of IoT applications:

Efficient and simple mechanisms for interaction with "things"

Design of simple methods (and their standardisation) that will enable application developers to include appropriate sensors, actuators and other "things" regardless of who designed and deployed them into applications without having to know the details of the implementation of each device. These should include not only communication methods, but also normalization of observations taking into account the conditions under which the observations were taken.

Reliable and trustworthy participatory sensing

Inclusion of humans in the loop and leveraging their mobility and the mobility of their personal communication devices to capture "snapshots" of the physical world on a global scale and create a "community wisdom" view of the physical world.

Creating knowledge and making it available

Creation and provision of services capable of processing and analysing massive data generated by communicating things ("making sense out of sensed data") with open interfaces that allow their simple integration into various applications.

Set up interdisciplinary projects for smart energy, grid and mobility

Smart grid and smart mobility topics each merge know how from very different disciplines (e.g. traffic management, urban management, automotive, communication). Specialists in the fields are "speaking different languages" and need to come to a mutual understanding. Ideally projects should go along

with show cases which could act as seeds for the new infrastructure. We need to address the challenges via a number of projects which are run by interdisciplinary consortia.

Foster Standardisation for smart energy, grid and mobility

Foster and promote international standardisation activities in order to allow for coherent infrastructures and to open the market for competition.

Support Public Awareness

Some aspects of the technologies discussed are critical with respect to privacy and they will have social implications because, e.g., they deal with private information or they might affect urban planning. Accompanying studies could help us to understand social consequences and to identify eventual show stoppers by time. Critical issues should be put for public discussion in an early phase in order to avoid later acceptance problems.

Seamless integration of social and sensor networks

Tools and techniques for the seamless integration of social networks and sensor networks, moving towards social IoT services that take into account the end-user's social preferences and interactions.

Infrastructures for social interactions between Internet-connected objects

Infrastructure, which could enable new forms of M2M interactions along with associated opportunities for innovative applications and services. Research could build upon existing semantic interactions and M2M APIs.

Utility metrics and utility driven techniques for "Clouds of Things"

Specification of utility metrics and utility driven techniques in the scope of "Clouds of Things".

2.12.2 Recommendations for Autonomic and Self-aware IoT

Self-awareness from the design to deployment

The IoT will exponentially increase the scale and the complexity of existing computing and communication systems. Autonomy is thus an imperative

property for the IoT systems to have. It should be considered from the very early phases of IoT systems implementations, from conception to deployment of devices, infrastructures and services. Self-awareness property should be injected to any software module, however separated from the functional code. Specific working groups on self-management issues should be created in standardisation organisations, industrial alliances and fora on IoT. A self-organising network (SON) for LTE of 3GPP is a good initiative that should be followed by other next generation network standards.

Real-life use cases

Characterisation of self-x properties in IoT context should be done based on real-life cross-domain use cases. Prototypes should be developed at early stages in order to validate the theoretical results by measuring the overhead that autonomy can bring to IoT systems. Novel methodologies, architectures, algorithms, technologies, protocols and programming paradigms should be developed taking into account IoT specific characteristics such as resource constraints, dynamic, un-predictive, error prone and lossy environments, distributed and real-time data handling and decision making requirements, etc.

Exploiting existing research

Existing fundamental research results from domains including artificial intelligence, biological systems, control theory, embedded systems and software engineering are necessary to build scientifically proven solid, robust and reliable solutions. Existing research may need to be tailored to the IoT context. In addition, multidisciplinary conferences and workshops should be organised to foster the interaction level between experts in those domains.

Security and privacy

Security and privacy issues should be considered very seriously since IoT deals not only with huge amount of sensitive data (personal data, business data, etc.) but also has the power of influencing the physical environment with its control abilities. Cyber-physical environments must thus be protected from any kind of malicious attacks. The IoT should autonomously tune itself to different levels of security and privacy, while not affecting the quality of service and quality of experience. Security attacks in autonomic and self-aware IoT systems in

safety context (e.g. driving cards) can become even more serious because the implementation of a security threat can impact the safety of a user by disrupting the autonomic process.

2.12.3 Infrastructure

IoT infrastructure as general infrastructure

More and more applications and services will rely on being directly connected to the physical world, i.e. for getting real-time information about the state of the real world or even for executing actuation tasks that directly influence the real world. Therefore, the IoT infrastructure needs to become a horizontal application-independent infrastructure like electricity, water or communications infrastructures today. This requires a strong research focus on the infrastructure itself, which takes requirements from the large variety of IoT-related application areas, but is not specific to any one of them.

Easy connection and extension of infrastructure

It has to be made easy to add IoT devices to the IoT infrastructure based on plugandplay type functionality, making additional configuration like semantic annotation easy for the user. This will require more standardisation activities on the protocol as at the information modelling level.

Core infrastructure services for supporting resolution, discovery, monitoring and adaptation

The infrastructure has to support the findings of relevant things and related services, enabling the connection to these services and facilitate the monitoring and adaptation of applications and services as a result of changes in the IoT infrastructure, i.e. with respect to the availability of IoT and related services.

2.12.4 Networks, Communications

2.12.4.1 Networks

Research on mobile networks and mobile networks of networks

A widespread introduction of Internet of Things devices will cause mobile devices at the access fringe of the mobile communication network to evolve

into their own mobile networks and even networks of networks. This predictable transition of the network structure has to become the topic of adequate research.

Research on load modelling of future IoT aware networks

In the emerging area of big data, related applications and widespread devices, sensors and actuators, predictive load modelling for the networks of the future will be essential for network optimization and pricing of network traffic, and it will influence the construction especially of such big data applications. The concurrent and synchronized development of all these fields is a field of challenging research.

Research on symbiosis of networking and IoT related distributed data processing

Large or global area applications will lead to a symbiosis of networking and distributed data processing. Generic architectures for this symbiosis, independent of specific applications, shall be researched, supporting data processing at the data sources, near to them or distributed randomly over the network.

IPv6 and large scale deployments of IoT components

The exponential number of smart things and the development of smart cities will require interconnecting very large number of devices and coping with unprecedented scale of network. In this context further research on the role of IPv6 to interconnect heterogeneous IoT components together with heterogeneous cloud applications is of high relevance. The development of a European research infrastructure enabling interconnection of various research labs working on IoT and IPv6 would strengthen the position of European research.

2.12.4.2 Communications

Adapting the IP Protocol Paradigm

It is a paradigm that the IP protocol defines the Internet. Recent advances show that IP can be implemented on resource constrained IoT devices, including IPv6 through its optimized 6LoWPAN version. However, the constraints of very small IoT devices may be so limiting that optimised non-IP protocols may have to be used to communicate with them. Thus, it remains a research

challenge to develop communications architectures that enable resource constrained devices to participate in the IoT while preserving the benefits of IP-based communications and application development.

Open communication architectures

Currently wireless communication standards are constructed to support the mobility of user devices. They use frame sizes of some milliseconds, implying a significant processing capacity at the user entities. Many classes of IoT devices neither use nor need this support, and they don't possess the required processing power. Methods to construct wireless mobile communications standards, open not only to constrained devices, but to all possible general communication modes in parallel at one time, shall be researched, also allowing integration of legacy system in a all-IP ecosystem.

Communication architectures for (highly) constrained devices

Constrained and highly constrained devices in the context of the IoT promise to open new applications with significant market relevance. Due to their importance the air interfaces of these devices and their communication architecture should be researched starting from the constraints of these devices and they should be especially optimized for such (highly) constrained devices over all relevant communication layers.

Formal construction and proof methods in communications

Formal construction and proof methods in communications promise to lay a foundation for formally verifiable and formally verified communication architectures including interoperability up to the networks of networks structure of the Future Internet including the IoT. Such formal methods combined with semantic processing shall be topics in research aiming at their adoption for the construction and design of the Future Internet and the IoT.

Real-time lightweight protocols and platforms

Lightweight protocols and platforms for the real-time interaction with Internet-connected objects, including their interactive visualization.

2.12.5 Processes

The ability to model IoT-aware business processes, with all the peculiarities of such processes, and the availability of related process execution engines will be a key for further adoption of IoT technologies in the enterprise and business world. Research targeting the convergence of IoT with BPM and the necessary tooling needs to be strengthened. In particular it is recommended to address the following topics:

Modelling of IoT-aware processes

Existing (business) process modelling languages need to be extended and standardized in a way to support the highly event-driven nature of IoT processes, to explicitly integrate the notion of physical entities and devices, to add parameters for quality of information, trust, and reliability, and to enable the (sometimes ad hoc) distribution of sub-processes.

Inherent unreliability of IoT-aware processes

As the data coming from IoT devices such as sensors cannot always be guaranteed to be accurate and the devices and related services can suddenly fail, it is important that data quality and quality of service parameters can be modelled in order to build "reliable-enough" systems.

Execution of IoT-aware processes

Modelled processes as described above need to be executed both on centralized process execution engines, but often also on small, constrained devices. This holds true particularly for sub-processes responsible for the behaviour of a set of IoT devices. To support such operations, very lightweight and efficient process execution engines are needed.

Large-scale distribution of process logic

IoT processes are widely distributed in nature; certain parts of the business logic are often executed on local devices. This ranges from simple filtering and aggregation to the execution of business rules or even completely autonomous behaviour of individual devices. The methods and frameworks need to be developed to manage such distributions of software, to decide what (sub-)

process is executed where, to monitor the systems, and to ensure that all parts always work in a safe operations envelope.

2.12.6 Data Information Management

In the context of Data Management, and the related and base technologies, there are some challenges and recommendations that should be considered as key elements to include in the Strategic Research and Innovation Agenda for the near future. Some of the topics with room for improvement or unresolved issues are:

Standardisation and Interoperability

Different technologies and components involved in data processing still use proprietary or ad-hoc protocols or data formats, making the exchange of data among different systems or the interconnection of components for a combined processing of the information (for instance, connecting a Data Collection and Analysis platform with a Data Mining solution) impossible or very complex. It is essential that data representation, interfaces and protocols are standardised or open, allowing a true "protocol independence" and interoperability.

Distribution, Federation and De-centralisation

Currently, most of the systems and platforms devised for acquisition, storage or processing of data are centralised and operated by a single administrator managing physical resources allocated in a very precise geographical location. No interconnection or distribution of data is permitted, thus limiting the possibilities for parallel or concurrent processing of data and also limiting the scope and domain of data that can be collected by the system. In the future, systems should have the capacity to be deployed and distributed geographically. A distributed system avoids or reduces the risk of failures and minimises the existence of bottlenecks in certain parts or features of the system. Federation policies, with reliable trust mechanisms, must be established to ensure that data can be accessed or exchanged remotely without compromising the integrity or security of involved data.

Data protection, Privacy and Security

When addressing data management, coming from very various sources and containing information on many different aspects, data security and privacy

aspects are critical. Different access levels, control policies, and mechanisms to guarantee that no identification of personal data is possible by unauthorised clients/operators must be carefully defined and applied. In addition, and depending on the use case or scenario, "opt-in" paradigms (in which users must voluntarily express and confirm their awareness and willingness to share personal data) should be incorporated as much as possible.

Improved semantics and Data Mining

Currently, the volume of data susceptible of being collected and automatically stored in information systems is huge. Often, the main problem is how to "understand" the information captured by the sensors or stored in the databases. The lack of "data interpretation" impedes the efficient processing of the information when searching for results or trying to extract useful information from the source data. A lot of effort must be devoted to the definition and implementation of semantics and rules making it easier to process the information. Data representation (within databases) and search/processing algorithms should be capable of handling higher levels of abstraction, closer to human interpretation and manipulation of information, and allowing the (automatic) generation or extraction of relationships among data components (making possible the definition of complex inference rules). In this sense, definition and processing of Complex Events (the whole CEP concept) is a field yet to be explored.

Data sharing and optimization techniques

Novel data sharing and optimization techniques for cloud-based IoT environments.

Publishing techniques for sensor data and from interconnected objects

Techniques for the publishing of data stemming from sensors and Internet-connected objects as Linked Data, including techniques for the integration of IoT with the Linked Open Data Cloud (LOD).

2.12.7 Security

Improved frameworks and mechanisms for trust relationships

Further research is required to develop improved frameworks and mechanisms to enable trust relationships to be established, maintained and assessed.

In IoT-centric scenarios, trust relationships are required between people, devices and infrastructures. Decentralised, self-configuring approaches (e.g., Trust Negotiation) are better suited to the IoT. New aspects like identity for sensor and smart objects and their integration in IdM frameworks are still a challenge.

Security against infrastructure disruption

As IoT becomes incorporated into national and critical infrastructure, there is a requirement to provide security against infrastructure disruption. Research is required into attack detection and recovery/resilience for IoT-specific threats, as well as management support such as situational awareness tools/techniques and decision making.

Privacy protection mechanisms

As much of the IoT involves personal information, privacy mechanisms must be developed that enable individuals to control the handling of personal information. Research is required to develop privacy protection mechanisms that enable data to be stored/processed without the content being accessible to others and to prevent information being inferred about individuals from IoT exchanges. Privacy, authentication and data ownership in the context of globally distributed IoT networks is another key area of research.

2.12.8 Device Level Energy Issues

Low power communication

Power consumption reduction of RF full-receiver should have a target much below 5 mW to enable very small form factor and long life-time battery. Targeting below 1 mW would then enable support from energy harvesting systems enabling energy autonomous RF communications.

Ultra-wideband

Ultra-wideband is not to be forgotten in the Internet of Things domain, as it provides a feature of great interest in addition to the communication itself, which is the ranging or indoor localization one [154]. Here, standardisation is also expected to arise and market development to come. Mature solutions are now available, and waiting for market deployment and public acceptance.

Solar and thermal energy harvesting

Thermoelectric materials' intrinsic efficiency should be improved in order to convert a higher part of the few mW of thermal energy available. This efficiency improvement will be mainly performed by using micro and nanotechnologies (such as superlattices or quantum dots). Similarly, photovoltaic cells should be efficiency improved to decrease photovoltaic cells' sizes and to harvest energy even in darker places for IoT devices.

Vibration energy harvesting

Vibration energy harvesters will have higher power densities in the future (from 10 μW/g to 30 μW/g) and work on a wider frequency bandwidth. We expect that vibration energy harvesting devices to be plug and play (PnP) and to be able to work in any vibrating environment, within 10 years.

2.12.9 Interoperability

2.12.9.1 Research on Dynamicity of Interoperability and Its Measurement

There will be plenty of heterogeneous IoT solutions, protocols and descriptions (e.g. semantics), research is needed to ensure a dynamic interoperability by more advanced adaptation (e.g. for protocols) and understanding different worlds (e.g. for semantics). New approach to interoperability measurements must be sought.

2.12.9.2 Validation of Standards

The very first step of new products intended to be placed, on the market comes from standards. Ambiguity in standards lead to non-interoperable products and any activities such as organising interoperability events to validate new standards must be pursued.

2.12.9.3 Development and/or Use of Well-defined Interoperability Methodologies

Cost and time associated to validate conformity to standards are high and all the more when no market proof methods are used. Use of standardised

methods and eventually development of new one(s) dedicated to IoT would help to reduce the costs, have timely IoT deployment while ensuring high level of quality and interoperability of IoT products. That would also to consider the full chain of activities leading to interoperability and not in fragmented solutions as it is today.

2.12.9.4 Development of Market Accepted Test Specifications

Like with standards, test specifications are very important "companion" documents or even standards to ensure common and non-ambiguous interpretation of IoT standards. There is still a lot of empiric approaches used today by the market, which lead to high cost, long delay and often not ensuring enough interoperability. Tests specifications must be drafted also using some techniques allowing maintenance, automation, reducing costs while limiting ambiguities. Special language and notation might be sought if standardised approaches cannot fit for IoT.

2.12.9.5 Enabling Multi Systems Integration

Developing research on multi systems integration is key to enable future European SMEs to integrate larger systems and solutions, and requires research on different models of IoT and IoT systems integration, taking into account IP and legacy sensors platforms.

2.12.10 Standardisation

Life-cycle approach towards standardisation

Standardisation should be viewed as only one activity in a life-cycle process that also includes preparatory regulatory and legislative activities, as well as post-standardisation activities towards certification and validation. Special care should be taken for understanding pre-standardisation impacts coming from the various applied sectors.

Increased influence from applied Internet of Things sector

As the Internet of Things represents a set of technologies and tools to support a number of different applied sectors with varying needs, standardisation efforts increasingly need to connect to those applied sectors and cannot

be done in isolation as a self-contained topic. In particular, attention should not only be paid to proper SDOs, but also to Special Interest Groups, various Industry Alliances, but also open communities which also drive technology development and set "de facto" standards in their particular applied domain.

Reduce technology fragmentation

Technology fragmentation is a feature of the Internet of Things, particularly on the device side. There is a need to drive further standardisation of device technologies in the direction of using standard Internet protocols and Embedded Web technologies including Internet of Things data semantics, with the purpose to achieve true interoperability and horizontalization. More attention need also be taken towards standardized and open tools for development of Internet of Things devices.

Open system for integration of Internet of Things data

It is necessary to ensure the efficient integration of Internet of Things data from devices in an open environment. This will require standardisation of Internet of Things data formats and semantics. Furthermore, tools and technologies are required to achieve sharing of Internet of Things data across applied domains, and standardisation should be considered as a means to ensure the open and secure availability of Internet of Things data and information.

Transparent interaction with third-party IoT infrastructures

Tools and techniques for transparently interacting with third-party IoT infrastructures (including standards-based architectures (OGC/SWE) and Internet of Things platforms (such as Pachube.com)).

2.12.11 Societal, Economic and Legal Issues

Accessibility

The complexity of user requirements resulting from personal characteristics and preferences, together with the variety of devices they might use, poses a problem of systems being non-inclusive for individual users that have non-mainstream needs. Accessibility of future IoT technologies will be a challenge that needs to be addressed.

Trust and Privacy

Users' privacy concerns about the accessibility and use of information captured by IoT devices and sensors is an important challenge, and users need to be assured that the future Orwellian Big Brother nightmare isn't becoming a reality. They must be enabled to understand and manage and control the exposure of their private and sensitive data. This also includes legislation ensuring individual privacy rights with respect to what kind of surveillance and information the authorities can employ and access.

Non-Repudiation

Things and IoT devices that have provided information or services need to be traceable and, in mission critical cases there may need to be means to detect the legal entity responsible for a thing.

Table 2.1. Future technological developments.

Development	2012–2015	2016–2020	Beyond 2020
Identification Technology	• Unified framework for unique identifiers • Open framework for the IoT • URIs	• Identity management • Soft Identities • Semantics • Privacy awareness	• "Thing/Object DNA" identifier
Internet of Things Architecture Technology	• IoT architecture developments • IoT architecture in the FI • Network of networks architectures • F-O-T platforms interoperability	• Adaptive, context based architectures • Self-* properties	• Cognitive architectures • Experimental architectures
Internet of Things Infrastructure	• Special purpose IoT infrastructures • Application specific deployment • Operator specific deployment	• Integrated IoT infrastructures • Multi application infrastructures • Multi provider infrastructures	• Global, general purpose IoT infrastructures • Global discovery mechanism
Internet of Things Applications	• Participatory sensing • Cheap, configurable IoT devices • IoT device with strong processing and analytics capabilities • Ad-hoc deployable and configurable networks for industrial use	• IoT in food/water production and tracing • IoT in manufacturing industry • IoT in industrial lifelong service and maintenance • IoT device with strong processing and analytics capabilities • Application capable of handling heterogeneous high capability data collection and processing infrastructures	• IoT information open market

(*Continued*)

Table 2.1. (*Continued*)

Development	2012–2015	2016–2020	Beyond 2020
Communication Technology	• Ultra low power chip sets • On chip antennas • Millimeter wave single chips • Ultra low power single chip radios • Ultra low power system on chip	• Wide spectrum and spectrum aware protocols	• Unified protocol over wide spectrum
Network Technology	• Self aware and self organizing networks • IoT — IPv6 integration • Sensor network location transparency • Delay tolerant networks • Storage networks and power networks • Hybrid networking technologies	• Network context awareness • IPv6- enabled scalability	• Network cognition • Self-learning, self-repairing networks • Ubiquitous IPv6-based IoT deployment
Software and algorithms	• Large scale, open semantic software modules • Composable algorithms • Next generation IoT-based social software • Next generation IoT-based enterprise applications • IoT-aware process modelling languages and corresponding tools • IoT complex data analysis • IoT intelligent data visualization • Hybrid IoT and industrial automation systems	• Goal oriented software • Distributed intelligence, problem solving • Things-to-Things collaboration environments • IoT complex data analysis • IoT intelligent data visualization • Hybrid IoT and industrial automation systems	• User oriented software • The invisible IoT • Easy-to-deploy IoT sw • Things-to-Humans collaboration • IoT 4 All • User-centric IoT

(*Continued*)

Table 2.1. (*Continued*)

Development	2012–2015	2016–2020	Beyond 2020
Hardware	• Multi protocol, multi standards readers • More sensors and actuators • Secure, low-cost tags (e.g. Silent Tags) • NFC in mobile phones • Sensor integration with NFC • Home printable RFID tags	• Smart sensors (bio-chemical) • More sensors and actuators (tiny sensors)	• Nano-technology and new materials
Data and Signal Processing Technology	• Energy, frequency spectrum aware data processing • Data processing context adaptable	• Context aware data processing and data responses	• Cognitive processing and optimisation
Discovery and Search Engine Technologies	• Distributed registries, search and discovery mechanisms • Semantic discovery of sensors and sensor data	• Automatic route tagging and identification management centres	• Cognitive search engines • Autonomous search engines
Power and Energy Storage Technologies	• Energy harvesting (energy conversion, photovoltaic) • Printed batteries • Long range wireless power	• Energy harvesting (biological, chemical, induction) • Power generation in harsh environments • Energy recycling • Wireless power	• Biodegradable batteries • Nano-power processing unit
Security, Privacy & Trust Technologies	• User centric context-aware privacy and privacy policies • Privacy aware data processing	• Security and privacy profiles selection based on security and privacy needs	• Self adaptive security mechanisms and protocols • Self-managed secure IoT

(*Continued*)

Table 2.1. (*Continued*)

Development	2012–2015	2016–2020	Beyond 2020
	• Virtualization and anonymisation • Scalable PKI based on hierarchical and Cross certification approaches • Lightweight key management for establishing trust relationships • Privacy by Design techniques, including data minimisation, identification, authentication and anonymisation	• Privacy needs automatic evaluation • Context centric security • Homomorphic Encryption • Searchable Encryption • Protection mechanisms for IoT DoS/DdoS attacks	
Material Technology	• SiC, GaN • Silicon • Improved/new semiconductor manufacturing processes/technologies for higher temperature ranges	• Diamond	• Graphen
Interoperability	• Use of mix of pragmatic empiric approach and advanced interoperability approaches • Cost of interoperability still high • Some certification programmes in place	• Optimized and market proof interoperability approaches used • Interoperability under stress as market grows • Cost of interoperability reduced • Several successful certification programmes in place	• Automated self-adaptable and agile interoperability
Standardisation	• IoT standardisation • M2M standardisation • Interoperability profiles • Application independent sensor and actuator semantics and profiles	• Standards for cross interoperability with heterogeneous networks • IoT data and information sharing	• Standards for autonomic communication protocols

Table 2.2. Internet of Things Research Needs

Research needs	2012–2015	2016–2020	Beyond 2020
Identification Technology	• Convergence of IP and IDs and addressing scheme • Unique ID • Multiple IDs for specific cases • Extend the ID concept (more than ID number) • Electro Magnetic Identification — EMID	• Beyond EMID	• Multi methods — one ID
IoT Architecture	• Extranet (Extranet of Things) (partner to partner applications, basic interoperability, billions-of-things)	• Internet (Internet of Things) (global scale applications, global interoperability, many trillions of things)	
Internet of Things Infrastructure	• Application domain-independent abstractions & functionality • Cross-domain integration	• Cross-domain integration and management • Large-scale deployment of infrastructure • Context-aware adaptation of operation	• Self management and configuration
Internet of Things Applications	• Incentives and trust issues in participatory sensing applications • Linked open data for IoT • Standardisation of APIs • IoT device with strong processing and analytics capabilities • Ad-hoc deployable and configurable networks for industrial use • Mobile IoT applications for IoT industrial operation and service/ maintenance	• IoT information open market • Mobile IoT applications for IoT industrial operation and service/ maintenance • Fully integrated and interacting IoT applications for industrial use	• Building and deployment of public IoT infrastructure with open APIs and underlying business models • Mobile applications with bio-IoT-human interaction

(*Continued*)

Table 2.2. (*Continued*)

Research needs	2012–2015	2016–2020	Beyond 2020
SOA Software Services for IoT	• Composed IoT services (IoT Services composed of other Services, single domain, single administrative entity) • Modelling and execution of IoT aware (business) processes • Quality of Information and IoT service reliability	• Highly distributed IoT processes • Semi-automatic process analysis and distribution	• Fully autonomous IoT devices
Internet of Things Architecture Technology	• Adaptation of symmetric encryption and public key algorithms from active tags into passive tags • Universal authentication of objects • Graceful recovery of tags following power loss • More memory • Less energy consumption • 3-D real time location/position embedded systems • IoT Governance scheme	• Code in tags to be executed in the tag or in trusted readers • Global applications • Adaptive coverage • Object intelligence • Context awareness • Cooperative position embedded systems	• Intelligent and collaborative functions
Communication Technology	• Longer range (higher frequencies — tenths of GHz) • Protocols for interoperability • Protocols that make tags resilient to power interruption and fault induction • Collision-resistant algorithms	• On chip networks and multi standard RF architectures • Plug and play tags • Self repairing tags	• Self configuring, protocol seamless networks
Network Technology	• Grid/Cloud network • Hybrid networks	• Service based network • Integrated/universal authentication	• Need based network • Internet of **Everything**

(*Continued*)

Table 2.2. (*Continued*)

Research needs	2012–2015	2016–2020	Beyond 2020
	• Ad hoc network formation • Self organising wireless mesh networks • Multi authentication • Sensor RFID-based systems • Networked RFID-based systems — interface with other networks — hybrid systems / networks • IPv6 enabled IoT and IPv6 European test bed for IoT	• Brokering of data through market mechanisms • Scalability enablers • IPv6-based networks for smart cities	• Robust security based on a combination of ID metrics • Autonomous systems for non stop information technology service • Global European IPv6-based Internet of Everything

Software and algorithms	• Self management and control
	• Micro operating systems
	• Context aware business event generation
	• Interoperable ontologies of business events
	• Scalable autonomous software
	• Software for coordinated emergence
	• (Enhanced) Probabilistic and non-probabilistic track and trace algorithms, run directly by individual "things"
	• Software and data distribution systems
		• Evolving software
		• Self reusable software
		• Autonomous things:
		  ○ Self configurable
		  ○ Self healing
		  ○ Self management
		• Platform for object intelligence
			• Self generating "molecular" software
			• Context aware software

Hardware Devices	• Paper thin electronic display with RFID • Ultra low power EPROM/FRAM • NEMS • Polymer electronic tags • Antennas on chip • Coil on chip	• Polymer based memory • Molecular sensors • Autonomous circuits • Transparent displays • Interacting tags • Collaborative tags	• Biodegradable antennas • Autonomous "bee" type devices

(*Continued*)

Table 2.2. (*Continued*)

Research needs	2012–2015	2016–2020	Beyond 2020
	• Ultra low power circuits • Electronic paper • Devices capable of tolerating harsh environments (extreme temperature variation, vibration and shock conditions and contact with different chemical substances) • Nano power processing units • Silent Tags • Biodegradable antennae	• Heterogeneous integration • Self powering sensors • Low cost modular devices	• Biodegradable antennas • Autonomous "bee" type devices
Hardware Systems, Circuits and Architectures	• Multi protocol front ends • Multi standard mobile readers • Extended range of tags and readers • Transmission speed • Distributed control and databases • Multi-band, multi-mode wireless sensor architectures • Smart systems on tags with sensing and actuating capabilities (temperature, pressure, humidity, display, keypads, actuators, etc.) • Ultra low power chip sets to increase operational range (passive tags) and increased energy life (semi passive, active tags) • Ultra low cost chips with security • Collision free air to air protocol • Minimum energy protocols	• Adaptive architectures • Reconfigurable wireless systems • Changing and adapting functionalities to the environments • Micro readers with multi standard protocols for reading sensor and actuator data • Distributed memory and processing • Low cost modular devices • Protocols correct by construction	• Heterogeneous architectures • "Fluid" systems, continuously changing and adapting

(*Continued*)

Table 2.2. (*Continued*)

Research needs	2012–2015	2016–2020	Beyond 2020
Data and Signal Processing Technology	• Common sensor ontologies (cross domain) • Distributed energy efficient data processing	• Autonomous computing • Tera scale computing	• Cognitive computing
Discovery and Search Engine Technologies	• Scalable Discovery services for connecting things with services while respecting security, privacy and confidentiality • "Search Engine" for Things • IoT Browser • Multiple identities per object	• On demand service discovery/ integration • Universal authentication	• Cognitive registries
Power and Energy Storage Technologies	• Printed batteries • Photovoltaic cells • Super capacitors • Energy conversion devices • Grid power generation • Multiple power sources	• Paper based batteries • Wireless power everywhere, anytime • Power generation for harsh environments	• Biodegradable batteries
Interoperability	• Innovative validation methodologies for IoT (eg test notation, MBT+) • Dynamic and adaptable interoperability for technical and semantic areas • Open platform for IoT validation	• Continuation 2015 research	• Self-adaptable and agile interoperability approaches
Security, Privacy & Trust Technologies	• Adaptation of symmetric encryption and public key algorithms from active tags into passive tags	• Context based security activation algorithms • Service triggered security	• Cognitive security systems • Self-managed secure IoT

(*Continued*)

Table 2.2. (*Continued*)

Research needs	2012–2015	2016–2020	Beyond 2020
	• Low cost, secure and high performance identification/ authentication devices • Quality of Information to enable reliable data processing • Assurance methods for trusted platforms • Access control and accounting schemes for IoT • General attack detection and recovery/resilience for IoT • Cyber Security Situation Awareness for IoT • Fine-grained self configuring access control to IoT • Ensuring end users that they are in control of their sensitive and private data • Trust Negotiation	• Context-aware devices • Object intelligence • Decentralised self configuring methods for trust establishment • Novel methods to assess trust in people, devices and data • Location privacy preservation • Personal information protection from inference and observation	• Decentralised approaches to privacy by information localisation
Societal responsibility	• Impact of IoT on environment, labour market, education, society at large • IoT also for underprivileged people	• Smart assistance by IoT in daily live	
Governance (legal aspects)	• Privacy and security legal analysis, framework and guidelines for IoT • Allocation and management of IPv6 addresses + RFID tags • Identifier uniqueness	• Legal framework for transparency of IoT bodies and organizations • Privacy knowledge base and development privacy standards	• Adoption of clear European norms/standards regarding Privacy and Security for IoT
Economic	• Business cases and value chains for IoT		
Material Technology	• Carbon • Conducting Polymers and semiconducting polymers and molecules • Conductive ink • Flexible substrates • Modular manufacturing techniques	• Carbon nanotube	• Graphen

Acknowledgments

The Internet of Things European Research Cluster (IERC) — European Research Cluster on the Internet of Things maintains its Strategic Research and Innovation Agenda (SRIA), taking into account its experiences and the results from the on-going exchange among European and international experts.

The present document builds on the 2010 and 2011 Strategic Research Agendas and presents the research fields and an updated roadmap on future research and development until 2015 and beyond 2020.

The IoT European Research Cluster SRA is part of a continuous IoT community dialogue supported by the European Commission (EC) DG Connect — Communications Networks, Content and Technology, E1 — Network Technologies Unit for the European and international IoT stakeholders. The result is a lively document that is updated every year with expert feedback from on-going and future projects financed by the EC.

Many colleagues have assisted over the last few years with their views on the Internet of Things Strategic Research and Innovation agenda document. Their contributions are gratefully acknowledged.

List of Contributors

Abdur Rahim Biswas, IT, create-net, iCore
Alessandro Bassi, FR, Bassi Consulting, IoT-A
Ali Rezafard, IE, Afilias, EPCglobal Data Discovery JRG
Amine Houyou, DE, SIEMENS, IoT@Work
Antonio Skarmeta, SP, University of Murcia, IoT6
Carlo Maria Medaglia, IT, University of Rome 'Sapienza', IoT-A
César Viho, FR, Probe-IT
Claudio Pastrone, IT, ISMB, Pervasive Technologies Research Area, ebbits
Daniel Thiemert, UK, University of Reading, HYDRA
David Simplot-Ryl, FR, INRIA/ERCIM, ASPIRE
Eric Mercier, FR, CEA-Leti
Erik Berg, NO, Telenor, IoT-I
Francesco Sottile, IT, ISMB, BUTLER
Franck Le Gall, FR, Inno, PROBE-IT, BUTLER
François Carrez, GB, IoT-I
Frederic Thiesse, CH, University of St. Gallen, Auto-ID Lab

Gianmarco Baldini, EU, EC, JRC
Giuseppe Abreu, DE, Jacobs University Bremen, BUTLER
Ghislain Despesse, FR, CEA-Leti
Hanne Grindvoll, NO, SINTEF
Harald Sundmaeker, DE, ATB GmbH, SmartAgriFood, CuteLoop
Jan Höller, SE, EAB
Jens-Matthias Bohli, DE, NEC
John Soldatos, GR, Athens Information Technology, ASPIRE, OpenIoT
Jose-Antonio, Jimenez Holgado, ES, TID
Klaus Moessner, UK, UNIS, IoT.est
Kostas Kalaboukas, GR, Singular Logic, EURIDICE
Lars-Cyril Blystad, NO, SINTEF
Latif Ladid, UL, IPv6 Forum
Levent Gürgen, FR, CEA-Leti
Mario Hoffmann, DE, Fraunhofer-Institute SIT, HYDRA
Markus Eisenhauer, DE, Fraunhofer-FIT, HYDRA, ebbits
Markus Gruber, DE, ALUD
Martin Bauer, DE, NEC, IoT-A
Martin Serrano, IE, DERI, OpenIoT
Maurizio Spirito, IT, Istituto Superiore Mario Boella, Pervasive Technologies Research Area, ebbits
Nicolaie L. Fantana, DE, ABB AG
Payam Barnaghi, UK, UNIS, IoT.est
Philippe Cousin, FR, easy global market, PROBE-IT,
Raffaele Giaffreda, IT, CNET, iCore
Richard Egan, UK, TRT
Rolf Weber, CH, UZH
Sébastien Boissseau, FR, CEA-Leti
Sébastien Ziegler, CH, Mandat International, IoT6
Stefan Fisher, DE, UZL
Stefano Severi, DE, Jacobs University Bremen, BUTLER
Srdjan Krco, RS, Ericsson, IoT-I
Sönke Nommensen, DE, UZL, Smart Santander
Trevor Peirce, BE, CASAGRAS2
Vincent Berg, FR, CEA-Leti
Vlasios Tsiatsis, SE, EAB

WolfgangKönig, DE, ALUD
WolfgangTempl, DE, ALUD

Contributing Projects and Initiatives

ASPIRE, BRIDGE, CASCADAS, CONFIDENCE, CuteLoop, DACAR, ebbits, ARTEMIS, ENIAC, EPoSS, EU-IFM, EURIDICE, GRIFS, HYDRA, IMS2020, Indisputable Key, iSURF, LEAPFROG, PEARS Feasibility, PrimeLife, RACE network RFID, SMART, StoLPaN, SToP, TraSer, WALTER, IoT-A, IoT@Work, ELLIOT, SPRINT, NEFFICS, IoT-I, CASAGRAS2, eDiana, OpenIoT, IoT6, iCore PROBE-IT, BUTLER, IoT-est, SmartAgriFood.

List of Abbreviations and Acronyms

Acronym	Meaning
3GPP	3rd Generation Partnership Project
AAL	Ambient Assisted Living
ACID	Atomicity, Consistency, Isolation, Durability
ACL	Access Control List
AMR	Automatic Meter Reading Technology
API	Application Programming Interface
AWARENESS	EU FP7 coordination action Self-Awareness in Autonomic Systems
BACnet	Communications protocol for building automation and control networks
BAN	Body Area Network
BDI	Belief-Desire-Intention architecture or approach
Bluetooth	Proprietary short range open wireless technology standard
BPM	Business process modelling
BPMN	Business Process Model and Notation
BUTLER	EU FP7 research project uBiquitous, secUre inTernet of things with Location and contExt-awaReness
CAGR	Compound annual growth rate
CE	Council of Europe
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Électrotechnique

CEO	Chief executive officer
CEP	Complex Event Processing
CSS	Chirp Spread Spectrum
D1.3	Deliverable 1.3
DATEX-II	Standard for data exchange involving traffic centres
DCA	Data Collection and Analysis
DNS	Domain Name System
DoS/DDOS	Denial of service attack Distributed denial of service attack
EC	European Commission
eCall	eCall — eSafety Support A European Commission funded project, coordinated by ERTICO-ITS Europe
EDA	Event Driven Architecture
EH	Energy harvesting
EMF	Electromagnetic Field
ERTICO-ITS	Multi-sector, public/private partnership for intelligent transport systems and services for Europe
ESOs	European Standards Organisations
ESP	Event Stream Processing
ETSI	European Telecommunications Standards Institute
EU	European Union
Exabytes	10^{18} bytes
FI	Future Internet
FI PPP	Future Internet Public Private Partnership programme
FIA	Future Internet Assembly
FIS 2008	Future Internet Symposium 2008
F-ONS	Federated Object Naming Service
FP7	Framework Programme 7
FTP	File Transfer Protocol
GFC	Global Certification Forum
GreenTouch	Consortium of ICT research experts
GS1	Global Standards Organization
Hadoop	Project developing open-source software for reliable, scalable, distributed computing
IAB	Internet Architecture Board
IBM	International Business Machines Corporation

ICAC	International Conference on Autonomic Computing
ICANN	Internet Corporation for Assigned Name and Numbers
ICT	Information and Communication Technologies
iCore	EU research project Empowering IoT through cognitive technologies
IERC	Internet of Things European Research Cluster
IETF	Internet Engineering Task Force
INSPIRE	Infrastructure for Spatial Information in the European Community
IoE	Internet of Energy
IoM	Internet of Media
IoP	Internet of Persons
IoS	Internet of Services
IoT	Internet of Things
IoT6	EU FP7 research project Universal integration of the Internet of Things through an IPv6-based service oriented architecture enabling heterogeneous components interoperability
IoT-A	Internet of Things Architecture
IoT-est	EU ICT FP7 research project Internet of Things environment for service creation and testing
IoT-i	Internet of Things Initiative
IoV	Internet of Vehicles
IP	Internet Protocol
IPSO Alliance	Organization promoting the Internet Protocol (IP) for Smart Object communications
IPv6	Internet Protocol version 6
ISO 19136	Geographic information, Geography Mark-up Language, ISO Standard
IST	Intelligent Transportation System
KNX	Standardized, OSI-based network communications protocol for intelligent buildings
LNCS	Lecture Notes in Computer Science
LOD	Linked Open Data Cloud
LTE	Long Term Evolution
M2M	Machine-to-Machine

MAC	Media Access Control data communication protocol sub-layer
MAPE-K	Model for autonomic systems: Monitor, Analyse, Plan, Execute in interaction with a Knowledge base
makeSense	EU FP7 research project on Easy Programming of Integrated Wireless Sensors
MB	Megabyte
MIT	Massachusetts Institute of Technology
MPP	Massively parallel processing
NIEHS	National Institute of Environmental Health Sciences
NFC	Near Field Communication
NoSQL	not only SQL — a broad class of database management systems
OASIS	Organisation for the Advancement of Structured Information Standards
OEM	Original equipment manufacturer
OGC	Open Geospatial Consortium
OMG	Object Management Group
OpenIoT	EU FP7 research project Part of the Future Internet public private partnership Open source blueprint for large scale self-organizing cloud environments for IoT applications
Outsmart	EU project Provisioning of urban/regional smart services and business models enabled by the Future Internet
PAN	Personal Area Network
PET	Privacy Enhancing Technologies
Petabytes	10^{15} byte
PHY	Physical layer of the OSI model
PIPES	Public infrastructure for processing and exploring streams
PKI	Public key infrastructure
PPP	Public-private partnership
Probe-IT	EU ICT-FP7 research project Pursuing roadmaps and benchmarks for the Internet of Things
PSI	Public Sector Information

PV	Photo Voltaic
QoI	Quality of Information
RFID	Radio-frequency identification
SASO	IEEE international conferences on Self-Adaptive and Self-Organizing Systems
SDO	Standard Developing Organization
SEAMS	International Symposium on Software Engineering for Adaptive and Self-Managing Systems
SENSEI	EU FP7 research project Integrating the physical with the digital world of the network of the future
SIG	Special Interest Group
SLA	Service-level agreement/Software license agreement
SmartAgriFood	EU ICT FP7 research project Smart Food and Agribusiness: Future Internet for safe and healthy food from farm to fork
Smart Santander	EU ICT FP7 research project Future Internet research and experimentation
SOA	Service Oriented Approach
SON	Self Organising Networks
SSW	Semantic Sensor Web
SRA	Strategic Research Agenda
SRIA	Strategic Research and Innovation Agenda
SRA2010	Strategic Research Agenda 2010
SWE	Sensor Web Enablement
TC	Technical Committee
TTCN-3	Testing and Test Control Notation version 3
USDL	Unified Service Description Language
UWB	Ultra-wideband
W3C	World Wide Web Consortium
WS&AN	Wireless sensor and actuator networks
WSN	Wireless sensor network
WS-BPEL	Web Services Business Process Execution Language
Zettabytes	10^{21} byte
ZigBee	Low-cost, low-power wireless mesh network standard based on IEEE 802.15.4

References

[1] Analysys Mason, "Imagine an M2M world with 2.1 billion connected things", online at http://www.analysysmason.com/about-us/news/insight/M2M_forecast_Jan2011/

[2] Casaleggio Associati, "The Evolution of Internet of Things", February 2011, online at http:// www.casaleggio.it/pubblicazioni/Focus_internet_of_things_v1.81%20-%20 eng.pdf

[3] J. B., Kennedy, "When woman is boss, An interview with Nikola Tesla", in Colliers, January 30, 1926.

[4] M. Weiser, "The Computer for the 21st Century," *Scientific Am.*, Sept., 1991, pp. 94–104; reprinted in *IEEE Pervasive Computing*, Jan.–Mar. 2002, pp. 19–25."

[5] K. Ashton, "That 'Internet of Things' Thing", online at http://www.rfidjournal.com/ article/view/4986, June 2009

[6] N. Gershenfeld, "When Things Start to Think", Holt Paperbacks, New York, 2000

[7] N. Gershenfeld, R. Krikorian and D. Cohen, *Scientific Am.*, Sept., 2004

[8] World Economic Forum, "The Global Information Technology Report 2012 — Living in a Hyperconnected World" online at http://www3.weforum.org/docs/Global_ IT_Report_2012.pdf

[9] "Key Enabling Technologies", Final Report of the HLG-KET, June 2011

[10] International Technology Roadmap for Semiconductors, ITRS 2012 Update, online at http://www.itrs.net/Links/2012ITRS/2012Chapters/2012Overview.pdf

[11] W. Arden, M. Brillouët, P. Cogez, M. Graef, *et al.*, "More than Moore" White Paper, online at http://www.itrs.net/Links/2010ITRS/IRC-ITRS-MtM-v2%203.pdf

[12] Frost & Sullivan "Mega Trends: Smart is the New Green" online at http://www.frost. com/prod/servlet/our-services-page.pag?mode=open&sid=230169625

[13] E. Savitz, "Gartner: 10 Critical Tech Trends For The Next Five Years" online at http://www.forbes.com/sites/ericsavitz/2012/10/22/gartner-10-critical-tech-trends- for-the-next-five-years/

[14] E. Savitz, "Gartner: Top 10 Strategic Technology Trends For 2013" online at http://www.forbes.com/sites/ericsavitz/2012/10/23/gartner-top-10-strategic-technology- trends-for-2013/

[15] P. C. Evans and M. Annunziata, Industrial Internet: Pushing the Boundaries of Minds and Machines, General Electric Co., online at http://files.gereports.com/ wp-content/uploads/2012/11/ge-industrial-internet-vision-paper.pdf

[16] H. Bauer, F. Grawert, and S. Schink, Semiconductors for wireless communications: Growth engine of the industry, online at www.mckinsey.com/

[17] ITU-T, Internet of Things Global Standards Initiative, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

[18] International Telecommunication Union — ITU-T Y.2060 — (06/2012) — Next Generation Networks — Frameworks and functional architecture models — Overview of the Internet of things

[19] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, et al., "Internet of Things Strategic Research Agenda", Chapter 2 in Internet of Things — Global Technological and Societal Trends, River Publishers, 2011, ISBN 978-87-92329-67-7

[20] Smart Santander, EU FP7 project, Future Internet Research and Experimentation, online at http://www.smartsantander.eu/

[21] H. Grindvoll, O. Vermesan, T. Crosbie, R. Bahr, et al., "A wireless sensor network for intelligent building energy management based on multi communication standards — a case study", ITcon Vol. 17, pg. 43–62, http://www.itcon.org/2012/3

[22] EU Research & Innovation, "Horizon 2020", The Framework Programme for Research and Innovation, online at http://ec.europa.eu/research/horizon2020/index_en.cfm

[23] Digital Agenda for Europe, European Commission, Digital Agenda 2010–2020 for Europe, online at http://ec.europa.eu/information_society/digital-agenda/index_en.htm

[24] Gartner, "Hype Cycle for Emerging Technologies", 2011, online at http://www.gartner.com/it/page.jsp?id=1763814

[25] D. Evans, "The Internet of Things — How the Next Evolution of the Internet Is Changing Everything", CISCO White Paper, April 2011, online at http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[26] EU 2012. The ARTEMIS Embedded Computing Systems Initiative, October 2012 online at http://www.artemis-ju.eu/

[27] Foundations for Innovation in Cyber-Physical Systems, Workshop Report, NIST, 2013, online at http://www.nist.gov/el/upload/CPS-WorkshopReport-1-30-13-Final.pdf

[28] IERC — European Research Cluster on the Internet of Things, "Internet of Things — Pan European Research and Innovation Vision", October, 2011, online at, http://www.theinternetofthings.eu/sites/default/files/Rob%20van%20Kranenburg/IERC_IoT-Pan%20European%20Research%20and%20Innovation%20Vision_2011.pdf

[29] O. Vermesan, P. Friess, G. Woysch, P. Guillemin, S. Gusmeroli, et al. "Europe's IoT Stategic Research Agenda 2012", Chapter 2 in The Internet of Things 2012 New Horizons, Halifax, UK, 2012, ISBN 978-0-9553707-9-3

[30] SENSEI, EU FP7 project, *D1.4: Business models and Value Creation*, 2010, online at: http://www.ict-sensei.org.

[31] IoT-I, Internet of Things Initiative, FP7 EU project, online at http://www.iot-i.eu

[32] Libelium, "50 Sensor Applications for a Smarter World", online at http://www.libelium.com/top_50_iot_sensor_applications_ranking#

[33] OUTSMART, FP7 EU project, part of the Future Internet Private Public Partnership, "OUTSMART — Provisioning of urban/regional smart services and business models enabled by the Future Internet", online at http://www.fi-ppp-outsmart.eu/en-uk/Pages/default.aspx

[34] BUTLER, FP7 EU project, online at http://www.iot-butler.eu/

[35] NXP Semiconductors N.V., "What's Next for Internet-Enabled Smart Lighting?", online at http://www.nxp.com/news/press-releases/2012/05/whats-next-for-internet-enabled-smart-lighting.html

[36] J. Formo, M. Gårdman, and J. Laaksolahti, "Internet of things marries social media", in *Proceedings of the 13th International Conference on Mobile HCI*, ACM, New York, NY, USA, pp. 753–755, 2011

[37] J. G. Breslin, S. Decker, and M. Hauswirth, *et al.*, "Integrating Social Networks and Sensor Networks", *W3C Workshop on the Future of Social Networking*, Barcelona, 15–16 January 2009

[38] M. Kirkpatrick, "The Era of Location-as-Platform Has Arrived", *Read Write Web*, January 25, 2010

[39] F. Calabrese, K. Kloeckl, and C. Ratti (MIT), "WikiCity: Real-Time Location-Sensitive tools for the city", in *IEEE Pervasive Computing*, July–September 2007

[40] N. Maisonneuve, M. Stevens, M. E. Niessen, L. Steels, "NoiseTube: Measuring and mapping noise pollution with mobile phones", in *Information Technologies in Environmental Engineering (ITEE 2009)*, Proceedings of the 4th International ICSC SymposiumThessaloniki, Greece, May 28–29, 2009

[41] J-S. Lee, B. Hoh, "Sell your experiences: a market mechanism based incentive for participatory sensing", *2010 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 60–68, March 29, 2010–April 2, 2010.

[42] R. Herring, A. Hofleitner, S. Amin, T. Nasr, A. Khalek, P. Abbeel, and A. Bayen, "Using Mobile Phones to Forecast Arterial Traffic Through Statistical Learning", *89th Transportation Research Board Annual Meeting*, Washington D.C., January 10–14, 2010.

[43] M. Kranz, L. Roalter, and F. Michahelles, "Things That Twitter: Social Networks and the Internet of Things", in *What can the Internet of Things do for the Citizen (CIoT) Workshop* at *The Eighth International Conference on Pervasive Computing (Pervasive 2010)*, Helsinki, Finland, May 2010.

[44] O. Vermesan, *et al.*, "Internet of Energy — Connecting Energy Anywhere Anytime" in Advanced Microsystems for Automotive Applications 2011: Smart Systems for Electric, Safe and Networked Mobility, Springer, Berlin, 2011, ISBN 978-36-42213-80-9

[45] W. Colitti, K. Steenhaut, and N. De Caro, "Integrating Wireless Sensor Networks with the Web," Extending the Internet to Low Power and Lossy Networks (IP+ SN 2011), 2011 online at http://hinrg.cs.jhu.edu/joomla/images/stories/IPSN_2011_koliti.pdf

[46] M. M. Hassan, B. Song, and E. Huh, "A framework of sensor-cloud integration opportunities and challenges", in *Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication*, ICUIMC 2009, Suwon, Korea, January 15–16, pp. 618–626, 2009.

[47] M. Yuriyama and T. Kushida, "Sensor-Cloud Infrastructure — Physical Sensor Management with Virtualized Sensors on Cloud Computing", NBiS 2010: 1–8.

[48] C. Bizer, T. Heath, K. Idehen, and T. Berners-Lee, "Linked Data on the Web", *Proceedings of the 17th International Conference on World Wide Web (WWW'08)*, New York, NY, USA, ACM, pp. 1265–1266, 2008.

[49] T. Heath and C. Bizer, "Linked Data: Evolving the Web into a Global Data Space", *Synthesis Lectures on the Semantic Web: Theory and Technology*, 1st edition. Morgan & Claypool, 1:1, 1–136, 2011.

[50] IBM, "An architectural blueprint for autonomic computing", IBM White paper. June 2005.

[51] "Autonomic Computing: IBM's perspective on the state of Information Technology", 2001, http://www.research.ibm.com/autonomic/manifesto/autonomic_computing.pdf

[52] International Conference on Autonomic Computing http://www.autonomic-conference.org/

[53] IEEE International Conferences on Self-Adaptive and Self-Organizing Systems, http://www.saso-conference.org/

[54] International Symposium on Software Engineering for Adaptive and Self-Managing Systems, http://www.seams2012.cs.uvic.ca/

[55] Awareness project, Self-Awareness in Autonomic Systems http://www.aware-project.eu/

[56] M. C. Huebscher, J. A. McCann, "A survey of autonomic computing — degrees, models, and applications", *ACM Computing Surveys (CSUR)*, Volume 40 Issue 3, August 2008.

[57] A. S. Rao, M. P. Georgeff, "BDI Agents: From Theory to Practice", in *Proceedings of The First International Conference on Multi-agent Systems (ICMAS)*, 1995. pp. 312–319.
[58] G. Dimitrakopoulos, P. Demestichas, W. Koenig, *Future Network & Mobile Summit 2010 Conference Proceedings.*
[59] John Naisbit and Patricia Aburdene (1991), *Megatrends 2000*, Avon.
[60] D. C. Luckham, *Event Processing for Business: Organizing the Real-Time Enterprise*, John Wiley & Sons, 2012.
[61] T. Mitchell, *Machine Learning*, McGraw Hill, 1997.
[62] O. Etzion, P. Niblett, *Event Processing in Action*, Manning, 2011.
[63] V. J. Hodgem, J. Austin, "A Survey of Outlier Detection Methodologies", *Artificial Intelligence Review*, 22(2), pages 85–126, 2004.
[64] F. Angiulli, and C. Pizzuti, "Fast outlier detection in high dimensional spaces" in *Proc. European Conf. on Principles of Knowledge Discovery and Data Mining*, 2002.
[65] H. Fan, O. Zaïane, A. Foss, and J. Wu, "Nonparametric outlier detection for efficiently discovering top-n outliers from engineering data", in *Proc. Pacific-Asia Conf. on Knowledge Discovery and Data Mining (PAKDD)*, Singapore, 2006.
[66] A. Ghoting, S. Parthasarathy, and M. Otey, "Fast mining of distance-based outliers in high dimensional spaces", in *Proc. SIAM Int. Conf. on Data Mining (SDM)*, Bethesda, ML, 2006.
[67] G. Box, G. Jenkins, *Time Series Analysis: Forecasting and Control*, Rev. ed., Oakland, California: Holden-Day, 1976.
[68] J. Hamilton, *Time Series Analysis*, Princeton Univ. Press, 1994.
[69] J. Durbin and S.J. Koopman, *Time Series Analysis by State Space Methods*, Oxford University Press, 2001.
[70] R. O. Duda, P. E. Hart, D. G. Stork, *Pattern Classification, 2nd Edition*, Wiley, 2000.
[71] C.M. Bishop, *Neural Networks for Pattern Recognition*, Oxford University Press, 1995.
[72] C. M. Bishop, *Pattern Recognition and Machine Learning*, Springer, 2006.
[73] M. J. Zaki, "Generating non-redundant association rules", *Proceedings of the Sixth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 34–43, 2000.
[74] M. J. Zaki, M. Ogihara, "Theoretical foundations of association rules", *3rd ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery*, 1998.
[75] N. Pasquier, Y. Bastide, R. Taouil, L. Lakhal, "Discovering Frequent Closed Itemsets for Association Rules", *Proceedings of the 7th International Conference on Database Theory*, (398–416), 1999.
[76] C. M. Kuok, A. Fu, M. H. Wong, "Mining fuzzy association rules in databases", *SIGMOD Rec.* 27, 1 (March 1998), 41–46.
[77] T. Kohonen, *Self-Organizing Maps*, Springer, 2001.
[78] S.-H. Hamed, S. Reza, "TASOM: A New Time Adaptive Self-Organizing Map", *IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics* 33(2): 271–282, 2003,
[79] L.J.P. van der Maaten, G.E. Hinton, "Visualizing High-Dimensional Data Using t-SNE", *Journal of Machine Learning Research* 9(Nov): 2579–2605, 2008.
[80] I. Guyon, S. Gunn, M. Nikravesh, and L. Zadeh (Eds), *Feature Extraction, Foundations and Applications*, Springer, 2006.
[81] Y. Bengio, "Learning deep architectures for AI", *Foundations and Trends in Machine Learning*, 2(1):1–12, 2009.

[82] Y. Bengio, Y. Le Cun, "Scaling learning algorithms towards AI", *Large Scale Kernel Machines*, MIT Press, 2007.

[83] B. Hammer, T. Villmann, "How to process uncertainty in machine learning?", *ESANN' 2007 Proceedings — European Symposium on Artificial Neural Networks*, Bruges (Belgium), 2007.

[84] J. Quinonero-Candela, C. Rasmussen, F. Sinz, O. Bousquet, and B. Schölkopf, "Evaluating Predictive Uncertainty Challenge", in *Machine Learning Challenges: Evaluating Predictive Uncertainty, Visual Object Classification, and Recognising Tectual Entailment*, First PASCAL Machine Learning Challenges Workshop (MLCW 2005), Springer, Berlin, Germany, 1–27, 2006.

[85] D. Koller and N. Friedman, *Probabilistic Graphical Models: Principles and Techniques*, MIT press, 2009.

[86] M. R. Endsley, "Measurement of situation awareness in dynamic systems", *Human Factors*, 37, 65–84, 1995.

[87] R. Fuller, *Neural Fuzzy System*, Åbo Akademi University, ESF Series A: 443, 1995, 249 pages. [ISBN 951-650-624-0, ISSN 0358-5654].

[88] S. Haykin, *Neural Networks: A Comprehensive Foundation*, 2nd edn., Prentice-Hall, New York (1999).

[89] L. Rabiner, "A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition," *Proceedings of the IEEE*, vol. 77, no. 2, Feb. 1989.

[90] S.K. Murthy, "Automatic construction of decision trees from data: A multi-disciplinary survey", *Data Mining Knowledge Discovery*, 1998.

[91] A. El Gamal, and Y-H Kim, *Network Information Theory*, Cambridge University Press, 2011.

[92] Z. Ma, "An Electronic Second Skin", in *Science*, vol. 333, 830–831 12 August, 2011

[93] Body Area Networks, IEEE 802.15 WPAN Task Group 6 (TG6), online at http://www.ieee802.org/15/pub/TG6.html

[94] M. Debbah, "Mobile Flexible Networks: Research Agenda for the Next Decade", 2008, online at http://www.supelec.fr/d2ri/flexibleradio/pub/atc-debbah.pdf

[95] S. Venkatesan, "Limits on transmitted energy per bit in a cellular wireless access network", Private communication, Radio Access Domain, Bell Labs, New Jersey, USA

[96] GreenTouch Consortium, online at www.greentouch.org

[97] GreenTouch, "Annual Report 2010–2011", online at http://www.greentouch.org/uploads/documents/GreenTouch_2010-2011_Annual_Report.pdf

[98] G. Rittenhouse *et al.*, "Understanding Power Consumption in Data Networks: A Systematic Approach", Eco. White paper, Alcatel-Lucent Bell Labs, Nov. 2009.

[99] A. Gluhak, M. Hauswirth, S. Krco, N. Stojanovic, M. Bauer, R. Nielsen, S. Haller, N. Prasad, V. Reynolds, and O. Corcho, "An Architectural Blueprint for a Real-World Internet", in *The Future Internet — Future Internet Assembly 2011: Achievements and Technological Promises*, Lecture Notes in Computer Science, Vol. 6656, 1st Edition, Chapter 3.3 Interaction Styles, 2011.

[100] G. Grov, Al. Bundy, C. B. Jones, and A. Ireland, "The Al4FM approach for proof automation within formal methods", Submission to *Grand Challenges in Computing Research 2010*, UKCRC, online at http://www.ukcrc.org.uk/grand-challenge/gccr10-sub-20.cfm

[101] C.A.R. Hoare, "Communicating Sequential Processes", Prentice Hall International, 1985 + 2004, ISBN 0131532715, and http://www.usingcsp.com/

[102] R. Milner, *Communicating and Mobile Systems: The π-calculus*, Cambridge University Press, 1999, ISBN 0-521-65869-1.

[103] S. Haller and C. Magerkurth, "The Real-time Enterprise: IoT-enabled Business Processes", IETF IAB Workshop on Interconnecting Smart Objects with the Internet, March 2011.

[104] OMG, Business Process Model and Notation specification, available at http://www.omg.org/technology/documents/br_pm_spec_catalog.htm, last accessed: November 15, 2011.

[105] OASIS, Web Services Business Process Execution Language, http://docs.oasis-open.org/wsbpel/2.0/wsbpel-v2.0.html, last accessed: November 15, 2011.

[106] W3C, Unified Service Description Language Incubator Group, online at http://www.w3.org/2005/Incubator/usdl/, last accessed: November 15, 2011.

[107] makeSense, EU FP7 Project, online at http://www.project-makesense.eu/, last accessed: November 15, 2011.

[108] J. Hellerstein, "Parallel Programming in the Age of Big Data", 2008, online at http://gigaom.com/2008/11/09/mapreduce-leads-the-way-for-parallel-programming/

[109] E. Dans, " Big Data: a small introduction", 2011, Retrieved from online at http://www.enriquedans.com/2011/10/big-data-una-pequena-introduccion.html.

[110] A. Sheth, C. Henson, and S. Sahoo, "Semantic sensor web", *Internet Computing*, IEEE, vol. 12, no. 4, pp. 78–83, July–Aug. 2008.

[111] Open Geospatial Consortium, Geospatial and location standards, http://www.opengeospatial.org.

[112] M. Botts, G. Percivall, C. Reed, and J. Davidson, "oGC Sensor Web Enablement: Overview and High Level Architecture", *The Open Geospatial Consortium*, 2008, online at http://portal.opengeospatial.org/files/?artifact id=25562

[113] W3C Semantic Sensor Network Incubator Group, Incubator Activity, online at http://www.w3.org/2005/Incubator/ssn/

[114] Semantic Sensor Network Incubator Group, State of the Art Survey, http://www.w3.org/2005/Incubator/ssn/wiki/State_of_the_art_survey.

[115] S. Decker and M. Hauswirth, "Enabling networked knowledge", in *CIA '08: Proceedings of the 12th international workshop on Cooperative Information Agents XII*, Berlin, Heidelberg: Springer-Verlag, pp. 1–15, 2008.

[116] P. Barnaghi, M. Presser, and K. Moessner, "Publishing Linked Sensor Data", in *Proceedings of the 3rd International Workshop on Semantic Sensor Networks (SSN)*, Organised in conjunction with the International Semantic Web Conference (ISWC) 2010, November 2010.

[117] Logical Neighborhoods, Virtual Sensors and Actuators, online at http://logicalneighbor.sourceforge.net/vs.html

[118] K. M. Chandy and W. R. Schulte, "What is Event Driven Architecture (EDA) and Why Does it Matter?", 2007, online at http://complexevents.com/?p=212, (accessed on: 25.02.2008).

[119] D. Luckham, "What's the Difference Between ESP and CEP?", 2006, online at http://complexevents.com/?p=103, accessed on 15.12.2008.

[120] The CEP Blog, http://www.thecepblog.com/

[121] EnOcean — the Energy Harvesting Wirless Standard for Building Automation and Industrial Automation, online at http://www.enocean.com/en/radio-technology/
[122] IEEE Std 802.15.4™-2006, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), online at http://www.ieee802.org/15/pub/TG4.html
[123] Bluetooth Low Energy (LE) Technology Info Site, online at http://www.bluetooth.com/English/Products/Pages/low_energy.aspx
[124] The Official Bluetooth Technology Info Site, online at http://www.bluetooth.com/
[125] M-G. Di Benedetto and G. Giancola, *Understanding Ultra Wide Band Radio Fundamentals*, Prentice Hall, June 27, 2004
[126] ISO, International Organization for Standardization (ISO), Identification cards — Contactless integrated circuit(s) cards — Vicinity cards, ISO/IEC 14443, 2003
[127] N. Pletcher, S. Gambini, and J. Rabaey, "A 52 μW Wake-Up Receiver With 72 dBm Sensitivity Using an Uncertain-IF Architecture", in *IEEE Journal of Solid-State Circuits*, vol. 44, no. 1, January, pp. 269–280. 2009.
[128] A. Vouilloz, M. Declercq, and C. Dehollain, "A Low-Power CMOS Super-Regenerative Receiver at 1 GHz", in *IEEE Journal of Solid-State Circuits*, vol. 36, no. 3, March, pp. 440–451, 2001.
[129] J. Ryckaert, A. Geis, L. Bos, G. van der Plas, J. Craninckx, "A 6.1 GS/s 52.8 mW 43 dB DR 80 MHz Bandwidth 2.4 GHz RF Bandpass Σ–Δ ADC in 40 nm CMOS", in *IEEE Radio-Frequency Integrated Circuits Symposium*, 2010.
[130] L. Lolis, C. Bernier, M. Pelissier, D. Dallet, and J.-B. Bégueret, "Bandpass Sampling RX System Design Issues and Architecture Comparison for Low Power RF Standards", *IEEE ISCAS 2010*.
[131] D. Lachartre, "A 550 μW inductorless bandpass quantizer in 65 nm CMOS for 1.4-to-3 GHz digital RF receivers", *VLSI Circuits 2011*, pp. 166–167, 2011.
[132] S. Boisseau and G. Despesse, "Energy Harvesting, Wireless Sensor Networks & Opportunities for Industrial Applications", in *EETimes*, 27th Feb 2012, online at http://www.eetimes.com
[133] J.G. Koomey, S. Berard, M. Sanchez, and H. Wong, "Implications of Historical Trends in the Electrical Efficiency of Computing", in *IEEE Annals of the History of Computing*, vol. 33, no. 3, pp. 46–54, March 2011.
[134] eCall — eSafety Support, online at http://www.esafetysupport.org/en/ecall_toolbox/european_commission/index.html
[135] European Commission,"Smart Grid Mandate, Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployments", M/490 EN,,Brussels 1st March, 2011.
[136] Global Certification Forum, online at http://www.globalcertificationforum.org
[137] SENSEI, EU FP7 project, online at http://www.sensei-project.eu
[138] IoT-A, EU FP7 project, online at http://www.iot-a.eu
[139] IoT6, EU FP7 project, online at http://www.iot6.eu
[140] IoT@Work, EU FP7 project, online at https://www.iot-at-work.eu/
[141] Federated Object Naming Service, GS1, online at http://www.gs1.org/gsmp/community/working_groups/gsmp#FONS
[142] Directive 2003/98/EC of the European Parliament and of the Council on the reuse of public sector information, 17 November 2003, online at http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive/psi_directive_en.pdf

[143] INSPIRE, EU FP7 project, — Infrastructure for Spatial Information in Europe, online at http://inspire.jrc.ec.europa.eu/
[144] H. van der Veer, A. Wiles, "Achiveing Technical Interoperability — the ETSI Approach", ETSI White Paper No. 3, 3rd edition, April 2008, http://www.etsi.org/images/files/ETSIWhitePapers/IOP%20whitepaper%20Edition%203%20final.pdf
[145] Ambient Assisted Living Roadmap, AALIANCE
[146] Atmel AVR Xmega Micro Controllers, http://it.mouser.com/atmel_xmega/
[147] Worldwide Cellular M2M Modules Forecast, Beecham Research Ltd, August 2010
[148] Future Internet Assembly Research Roadmap, FIA Research Roadmap Working Group, May 2011
[149] D. Scholz-Reiter, M.-A. Isenberg, M. Teucke, H. Halfar, "An integrative approach on Autonomous Control and the Internet of Things", 2010
[150] NIEHS on EMF, http://www.niehs.nih.gov/health/topics/agents/emf/
[151] R.H. Weber/R. Weber, *Internet of Things — Legal Perspectives*, Springer, Berlin 2010.
[152] "The Global Wireless M2M Market", Berg Insight, 2010, http://www.berginsight.com/ReportPDF/ProductSheet/bi-gwm2m-ps.pdf
[153] M. Hatton, "Machine-to-Machine (M2M) communication in the Utilities Sector 2010–2020", Machina Research, July 2011.
[154] G. Masson, D. Morche, H. Jacquinot, and P. Vincent, "A 1 nJ/b 3.2–4.7 GHz UWB 50 M pulses/s Double Quadrature Receiver for Communication and Localization", in *ESSCIRC 2010.*

This page intentionally left blank

3

IoT Applications — Value Creation for Industry

Nicolaie L. Fantana[1], Till Riedel[2],
Jochen Schlick[3], Stefan Ferber[4], Jürgen Hupp[5],
Stephen Miles[6], Florian Michahelles[7], and Stefan Svensson[8]

[1]*ABB CRC, Germany*
[2]*KIT TECO, Germany*
[3]*DFKI, Germany*
[4]*Bosch Software Innovations, Germany*
[5]*Fraunhofer IIS, Germany*
[6]*MIT, Auto-ID Labs, USA*
[7]*ETH, Auto-ID Labs, Switzerland*
[8]*ABB CRC, Sweden*

Abstract

IoT in industry is a rapidly developing area. Numerous IoT research and application projects have been done by universities or in joint industry-university consortia in recent years. However an important question to be further addressed is on value creation by IoT industry applications. IoT applications in the sense of this paper are solutions using IoT technologies to improve industrial manufacturing processes, enable new and efficient ways to operate production plants, create new service or supervision means for industrial installations, offer an optimized infrastructure, reduce operational cost or improve human safety in industrial areas. The present paper brings together

Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, 153–206.
© 2013 *River Publishers. All rights reserved.*

experts from academia, research and industry offering a view on the IoT application in industrial environment, the challenges, expected evolution of IoT technology and use in future factories, on connected and holistic processes. The paper is intended to contribute to an IoT supported paradigm change in manufacturing, industrial service and over life sustainable industrial activities.

3.1 Introduction

Internet of things (IoT) has become part of your daily life. The "things connected to the internet" idea is continuously evolving in content, areas of applications, visions and technology. New real life and industrial projects have been done and joint future oriented industry and government initiatives such as Industry 4.0 in Germany, have been started [1].

Since Industrial production is one of the world's biggest economic factors one of the major objectives of these initiatives is to bring the paradigms of the IoT to the factories enabling them to cope with the challenges raised by popular megatrends. The foremost megatrends relevant for factories are globalization, progressing technological evolution, the dynamization of product life cycles, the aging work force and the shortage of resources. Central effects are the acceleration of innovation cycles and the increasing customer demand for individualized mass produces with highest quality expectations.

Within the context of industrial production IoT projects and applications are developing in manufacturing, supply chain, supervision and servicing. A major question in all projects is about the value, the benefit such application can bring to the user, to the owner or to society.

The value question is extremely pertinent in the industry: in the manufacturing industry entire factory related processes, but also in industrial applications where it comes to ensure operation of industrial installations and provide supervision, and improved life service. It is the value which such applications bring which will determine their adoption, acceptance and wide use. However, this value is very difficult to quantify and prove, and it depends on multiple aspects which are strongly application area dependent.

The present paper is focusing on IoT applications form the point of view of value creation for industry and brings together expert opinions from academia, research and industry. The industrial application of IoT is multi- facetted and each of the subsections in this paper will highlight an aspect related to industrial

application, discuss or show a case or the evolution and potential of a specific technology from industry application point of view. The paper is having a holistic manner to industrial challenges and requirements. Also it will refer to factory concepts and applications supported by IoT, including processes and flows taking a view on related technologies and their evolution. These types of topics have been also addressed by the authors during an industrial workshop at a recent international conference [2].

At the beginning the paper presents a view form industry regarding IoT applications, the requirements and challenges which have to be overcome or capabilities expected form industrial IoT applications. Subsequent sections discuss items like: future factory concepts and experience in the area, evolution and future of IoT technologies, use of smart objects for creating smart IoT-based applications, technologies inspiring connected life related to industry. A view on the whole chain and flows and information services based on smart objects are presented followed by a shopping basket approach from industry view. Aspects from a real industrial application in the hard environment of oil and gas industry are presented. Some collected opinions on IoT and value aspects, obtained at an industry workshop during the 3rd IoT conference [2] are also shown.

3.2 IoT Applications for Industry — Value Creation and Challenges

IoT Applications

Throughout the entire document the following pragmatic definition for IoT applications was used in order to focus the scope and to have a common understanding: IoT applications in the sense of this paper are solutions using IoT technologies capable to improve and easy adapt industrial manufacturing processes, enable new and efficient ways to do operate and interact in production plants, create new service or supervision means for industrial installations, offer an optimized infrastructure, reduce operational cost and energy consumption or improve human safety in industrial areas.

Value, Benefit

To start a project in industry environment the expected benefit, the expected value to the company has to be estimated and later needs to be re-evaluated and

proved during operation. To define the value of an industrial IoT application or IoT project is difficult. There are numerous reasons for that. The value typically shows up gradually with new process introduction and accumulates over time, the value is often difficult to quantify due to multiple interactions and complex processes, it may contain hard but also soft benefits difficult to assess. Value can be generated and may show up as a result of a combination of IoT applications with other systems or processes, or can originate in new human behavior or new interactions. Fact is that value is the key element finally asked by the project stakeholders or owners.

There is agreement that IoT brings benefit in different areas, however numbers to quantify that value are scarce. More recently CISCO proposed a view called Internet of everything based on IoT and additionally "connecting to internet everything not connected yet" [3]. The global potential, the "value at stake", for what was called Internet of Everything economy and for the decade 2013–2022, was estimated to $14.4 trillion. Also 5 major drivers have been identified n [3] and 4 of them: asset utilization, productivity, logistics efficiency, innovation have strong connections with IoT applications in industry.

IoT applications benefit and value creation in an industrial environment may have its origin in different aspects, depending on the application type. There is no value but "values" each contributing to the total benefit such as:

- Value from visibility identification, location tracking
- Value form IoT-supported safety in hard industrial environments
- Value from right information providing or collecting
- Value form improved industrial operation and flows in industry
- Value from reduced production losses
- Value from reduced energy consumption
- Value from new type of processes made possible by IoT applications
- Value form new type of maintenance and lifetime approaches
- Value enabled by smart objects, connected aspects
- Value from sustainability.

The value form visibility was analyzed in a recent 2012 study by Forrester Research [4]. Based on the responses from this study and cumulating the responses "very important to bring value" and "important to bring value" the results are shown in Figure 3.1. The most important IoT technologies perceived

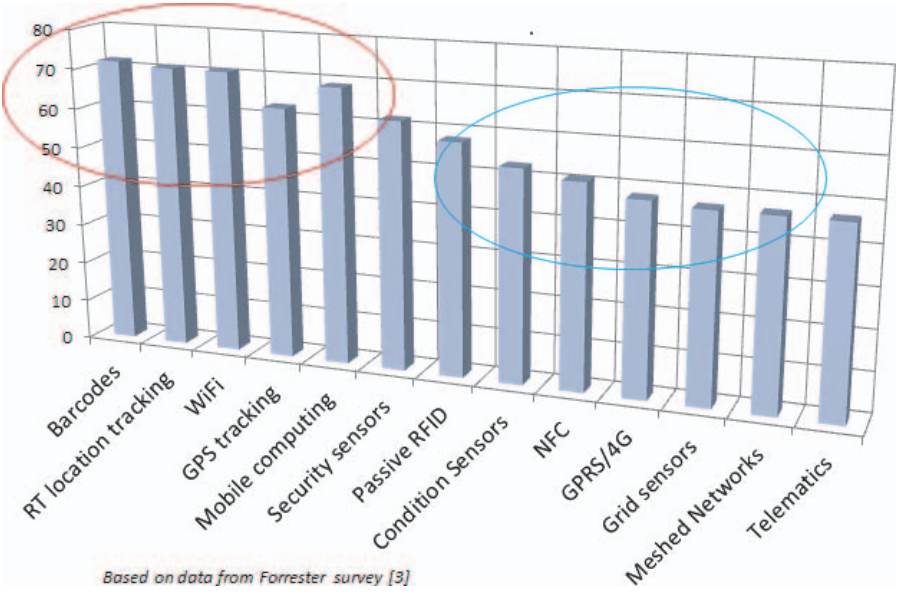

Fig. 3.1 View on very important and important perceived IoT technologies expected to bring value in applications.

by companies, as of 2012 study, are related to barcodes, tracking and mobile computing — the red border area, however RFID and NFC technologies, as well as sensors stand alone or meshed — the blue border area, are important too and show future potential.

The status and estimated potential of IoT applications is presented in Figure 3.2 considering three major areas: supply chain, future industry/future factory and over lifetime applications and activities such as logistics, manufacturing and service/maintenance. A strong potential and additional application is expected in industry operation and industry lifetime applications including lifetime service.

IoT applications requirements and capabilities

The expectations toward IoT applications in industry are high. The capabilities they have to offer are depending strongly on the industrial area and the concrete application. For example the environment where IoT application may be used may range from clean room condition and normal ambient temperatures to heavy and dirty environment, locations with high temperatures, areas with

Areas	Supply chain	Industry	Lifetime
Activities	Logistics	Manufacturing	Service
IoT **present** Applications and Value	Many	Some	Few
IoT **additional** Applications **Potential**	Increase	Strong	Strong

Fig. 3.2 Status and estimated potential of IoT applications.

explosion risk, areas with metallic surroundings, and corrosive environment on sea or underground.

A list of a set of industry related capabilities and requirements is presented below, without claiming completeness. The list items are related to the IoT hardware, software and to serviceability and management aspects. Comments have been added to all items to make the requirement more specific. The IoT application capabilities for industrial application should meet requirements such as:

- Reliability.
  Reliable IoT devices and systems should allow a continuous operation of industrial processes and perform on-site activities.
- Robustness.
  The IoT application and devices should be robust and adapted to the task and hard working conditions. This should include also the certifications for the specific work environment where they are used.
- Reasonable cost.
  Cost aspects are essential and should be fully justifiable and adapted to the benefit. It is basically about the right balance between cost and benefit rather than low cost. Also the costs are related to a more holistic view and life costs and consider the impact on the whole industrial installation in case of a failed IoT device or application.

- Security and safety.
  Security requirements are related to the cyber security threats and have to be part of the entire security strategy of the company.
  Safety is mainly related to the device construction and the area of use but also to usability such that no safety threats occur due to use of the IoT applications and devices.
- Simple use.
  Simple, intuitive use and (almost) self-explaining are important for the overall IoT application acceptance. The IoT application should ideally be context aware and adapt to the skills of the user and location or environment aspects.
- Optimal and adaptive set of features.
  The IoT application should allow to perform desired task with the sufficient, not-richer-then-necessary, set of features
- Low/No maintenance.
  Maintenance free or reduced maintenance IoT applications and devices over operational life would be ideal. Maintenance over lifetime is an important aspect impacting the life cycle costs of IoT based solutions. It is affected by the sometimes high number of IoT devices in place, the fact that they are typically distributed over large areas, the required skills, tools and time needed for any type of IoT maintenance operation. This is valid for all devices but especially for active IoT devices or active wireless sensing.
- Standardization.
  IoT devices and applications should be using a set of standards to support interoperability of IoT devices, easy exchange and multi-vendor possibilities.
- Integration capabilities.
  Easy integration in the IT and automation and process landscape of the industrial plant are required and may decide if a IoT solution will be used. This is particularly important for brown-field projects but also for green field in the view of future plant extensions.
- Reach sensing and data capabilities.
  IoT applications will relay more and more on complex sensing allowing distributed supervision and data collection and data capabilities. This is a chance in terms of additional data and

real-time information but also a challenge in terms of data and processing.

- Industry grade support and services.
  The IoT applications should be supported over years in operation by a set of rich tools and continuously updated services. Typically industry application requires also a centralized management of devices and systems, managed access rights, this might apply to some of IoT devices too.

Presently there are also numerous challenges to reach all the above.

Challenges faced by IoT industry applications

The challenges for IoT industrial applications can be subject of a more extended treatment, however for the needs of present IoT applications and value creation they have been divided in 4 groups:

- IoT device technical challenges
- Lifetime and energy challenge
- Data and information challenge
- Humans and business

The IoT devices technical challenges are numerous and subject of intense research. Some aspects will be addressed also in the following sections. A set of technical features will be especially needed in industrial applications, depending on application, such as extended capabilities for sensing in terms of sensor types and high sampling rate, communication, wireless data transfer and precise time synchronous collection of data both in single-hop and multi-hop industrial networks. Another aspect is related to the easy deployment, configuration and re-use of non-permanently attached devices, such as the ones used for ad-hoc sensing. One critical and often neglected aspect is the device packaging for the industrial application needs which is essential for reliable operation.

Last but not least is the heterogeneity aspect which is a problem even today. In industrial environments often encountered are combinations of one or more of: of passive and active RFID with or without sensing, various fix or mobile RFID readers, wireless sensor nodes and networks, wired and wireless technologies in factory automation, use of different frequency bands

13.5 MHz, 433 MHz, 860–925, 2.4 GHz, use of various "languages" — ISO standards, and different mobile devices and ecosystems.

A special challenge related to IoT devices is related to lifetime of the IoT device which is less than of the normal industrial installation. This lifetime mismatch needs to be considered in the complete design and management of industrial installations involving IoT. The energy challenge is also important, especially for active IoT devices. Depending on application the energy harvesting can be a solution.

A very important aspect is the data and information challenge. The IoT devices are important sources of rich and spatial distributed identification, historical and sensor data in industrial environment. With the advent of more intensive use in industry and taking as an example an industrial supervision case the data amounts can really explode. Taking a simple industry sensing and supervision example with 100 sensors installed and collecting sensing data such as: temperature 1 per min, 3axes acceleration data with 10 k samples per second, and 1 audio channel with say 40 ksamples per second, also considering that data is collected only 1% of daytime, approx. 15 min per day, the total amount of raw data for 1 year sums up to 4.4 PB/year. This is only to show that such amounts of raw data need to be processed and condensed and analyzed in order to be usable at all so not data but information behind it needs to be extracted for industrial use. Adaptive data handling and data processing and data fusion methods are required to handle also the industrial IoT data emerging, and will require new methods to visualize or inform about the status of real world. Also in industry the IoT data need to be correlated to the already available automation and control data in industrial plants. This blended information will be needed for a specific installation and typically on site too. All this data and information need also special attention regarding handling and management in terms of security and access.

Another challenge and one visible in the industrial megatrends is that technology in today's and future factories has to support the human more and more. Ageing work force and the lack of skilled people in combination with the increasing productivity, quality and cost pressure lead to the need to effectively utilize the unique human capability of purposeful behavior [5]. IoT technologies can help to support the humans and to disburden them from doing hard routine work or wasting their time searching for information.

An important aspect why IoT applications are not as wide-spread as desired is related to human and business aspects. Besides technical challenges there is a lack of business models usable in industrial environment, the business models behind the IoT applications. New types of industrial and business processes for operation and for servicing machineries have to be put in place, considering IoT technologies supported approaches which otherwise would not have been possible. It is also challenging to integrate new IoT applications into existing running and producing plant systems with minor drawbacks – to handle brown field applications.

Human resources and skills remain essential and are also a major factor in the new IT and IoT rich industrial environment. The challenges are related to scarce resources, to the complex blend of skills needed by persons on site in a future plant, and by the aspects related to the increasing complexity and knowledge needed for industrial installations.

From an industry point of view value creation form IoT applications and sustainability are essential. How these problems will be addressed and solved will influence the use of IoT technologies in the industry, on a larger scale, in the coming years. There is a continuously evolving process both in technology and applications and new future plant, future service and supervision solutions will emerge.

3.3 Future Factory Concepts

3.3.1 Lever Mechanisms for the IoT in Future Factories

The term "Internet of Things" describes a wide variety of concepts and applications in the context of equipping everyday items with computing and networking resources. Even if a common definition of the IoT might not exist, IoT implementations mainly focus three aspects (Figure 3.3): First, the network and addressability aspect. Real world objects are equipped with a computing and communication core and connected to each other. The focus is on high resolution data acquisition. Second, the ambient intelligence aspect. The network of intelligent objects realizing control loops. The focus is on control. Third, the ambient assistance aspect. High resolution data acquisition and ubiquitous computing are used to offer context sensitive services to the human [6]. This clearly focusses the human.

Image available in original Version

The network aspect offers open communication standards reaching down to the sensor-actuator level of today's factories and the distribution of control intelligence into equipment, infrastructure and products themselves. From a visionary point of view every item in future factories will be equipped with a computing and communication core. Communication allows delivering a detailed and actual virtual representation of the current state of the complete factory.

Standardized communication interfaces and distributed control intelligence within a factory internet lead to the fact that fine grained and actual information about products, equipment, technological and even organizational processes will basically be available at any time and everywhere within the factory. While this is miles away from today's state of the art in factories the mere availability of information does not create any added value by itself. The availability of information is only the basis for the optimization of technological and organizational processes. The optimization itself has to be initiated and conducted by humans.

This consideration leads to the insight that for future factory concepts the rather technical IoT aspects of networking and communication are only means to an end. The added value of IoT applications emerges out of the fact that humans can take advantage out of the availability of information and the

interoperability of devices. This means that the ambient assistance aspect of the IoT is the one that will be the basis for optimization of future factory processes and that will lead to a number of use cases. Future factory concepts based on the IoT will need to be human centered. The core element is to release the human operator, engineer or manager from doing routine work. Instead humans will be able to concentrate on their unique capability of defining the right strategy and defining the right goals to operate the factory effectively within the triangle of tension between costs, quality and output.

In this context the ambient intelligence aspect gets a new meaning. Following the nature of the IoT of making information available, ambient intelligence is the instrument to release the human from routine tasks concerning information retrieval and analysis. Autonomous behavior results from the defined reaction of equipment or infrastructure to the results of this analysis. So autonomy of equipment is no contradiction to the need of deterministic behavior at all.

3.3.2 The SmartFactory^{KL} Initiative

In order to transfer the central paradigms of the IoT to factory automation, many technologies working well in the consumer world have to be applied under industrial conditions. One of the biggest obstacles keeping responsibles away from the application of new technologies is missing trust and the lack of best practice examples.

For this reason in 2004, a group of people from industry and academia met and formulated the vision of a smart factory of the future. After feasibility study the technology initiative SmartFactory^{KL} was founded in 2005 as a public private partnership. Its target is to develop, apply and distribute innovative industrial plant technology. The founding partners represented various industry sectors. Meanwhile the number of partners has grown up to 22, including mainly partners from industry as well as universities and research centers. The funding is based on membership fees and public research projects given by German ministries and the EU [10].

The basic equipment of the SmartFactory^{KL} is an automated production facility for liquid colored soap (Figure 3.4). It contains a process manufacturing part as well as a piece handling part. Based on state of the art automation technology the equipment demonstrates the migration path to the application

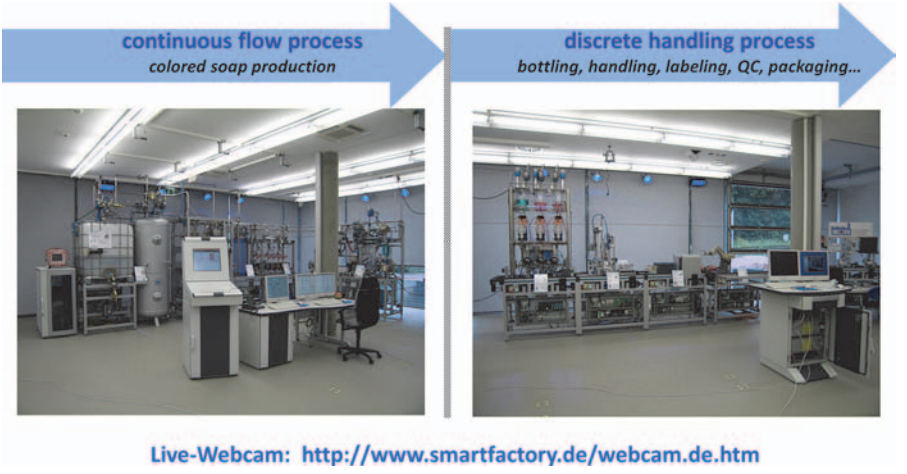

Fig. 3.4 SmartFactory^{KL} production facility.

of smart technologies in factory environments. In the meanwhile several additional demonstration modules have been set up showing the application of new technologies and paradigms like Service Oriented Automation architectures, Digital Product Memories, Plug&Play automation, Dynamic orchestration of automated processes and the use of tablet computers in industrial environments.

3.3.3 From Technologies to Technology Concepts

Often the discussion about the IoT in the context of industry applications is of technological nature. However, as stated before technology is only a means to an end. Experience with the SmartFactory^{KL} shows that instead of losing oneself in the discussion of technical implementation details one should focus on the application type of IoT technology. Regarding the future factory this are basically the smart product, the smart equipment, the smart infrastructure and the augmented operator. These concepts can be implemented using a wide range of technology depending on the concrete scenario.

3.3.3.1 Smart products

One of the approaches to connect the different information layers of a factory is to take advantage of the product itself as information carrier. Such a smart product primarily stores information about its production history and can

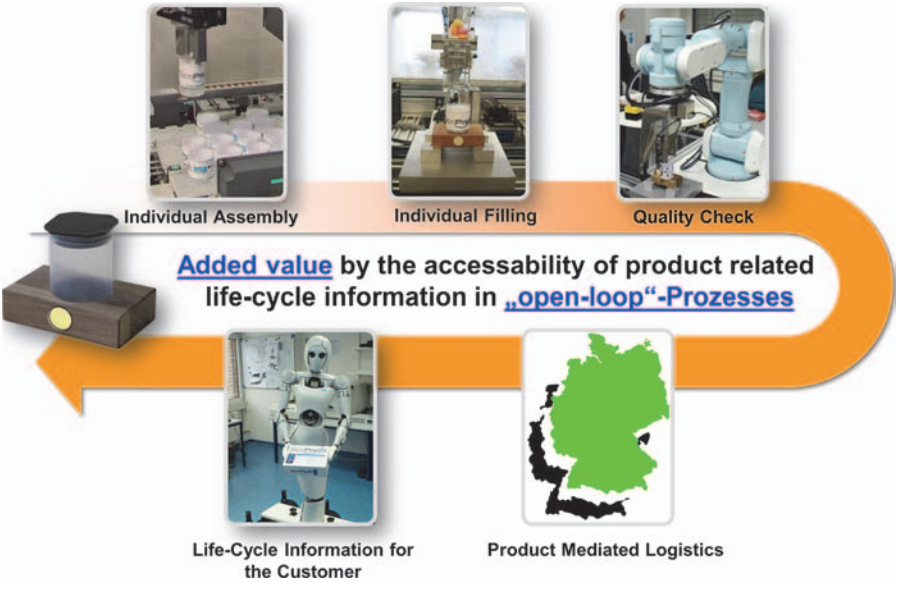
Individual Assembly
Individual Filling
Quality Check
Added value by the accessability of product related life-cycle information in „open-loop“-Prozesses
Life-Cycle Information for the Customer
Product Mediated Logistics

Fig. 3.5 Digital product memories in open-loop processes.

actively adapt its production sequence based on the current status of production (Figure 3.5). Another feature is the capability to realize a tight monitoring of events influencing the smart product. Basic elements are the memory itself and a software component that allows accessing and interpreting the stored information [9].

It is obvious that smart products can be implemented by applying an embedded system to the product itself. However there are many scenarios this is not really reasonable, either for cost, for size or for physical reasons given by the production process such as heat treatment or electrical discharge machining. Therefore the implementation often incorporates infrastructure such as barcode- or RFID Readers and backend server systems enabling to tag the product with robust and cheap items like bar- or data matrix codes or RFID Tags.

Using auto-ID tags means that the smartness is only enabled only during specific time frames of the active production phases by a complementary infrastructure. The complementary infrastructure allows the accessing of the product's on-board information and couples it with the logical border components. For example these "smart characteristics" are active only in the

time-frame before a product enters the assembly process, during which it determines the most appropriate assembly station. For most production processes this is not really a disadvantage since the equipment processing or transporting smart products typically has access to the backend infrastructure. Even containers or stores can be equipped with the respective means to access backend server systems.

3.3.3.2 Smart equipment and smart infrastructure

Smart equipment and smart infrastructure in future factories are characterized by two major features. First they will be networked. Second they will come with a certain degree of autonomy where networking enables to react on a wide range of context events. The ultimate goal of the smart equipment is to autonomously determine the appropriate processing tasks (e.g., a suitable machining strategy) to compensate failures and to communicate its production states and work-loads with the other production components. The autonomy level will mainly be enabled by reacting on the equipment's context. The smart infrastructure captures and communicates the environmental changes, like temperature, vibration or the location of the production components within the factory. While smart infrastructure primarily focusses the network aspect, smart equipment more focusses the autonomy aspect.

The aspect of networking has to be defined in a more general manner as it is realized today. Today's networks primarily enable the transport of data. The meaning of this data is typically hardcoded in the applications following some paper definitions. Many industrial networks define such information models for the typical application field such as motion control or real time IO. However networking in the context of the IoT describes the technology independent ad hoc communication of self-describing data. This means that the communication partners are not known at the design time of the network and that the underlying information models describing the meaning of data have to be made explicit and included within the communication protocol. OPC-UA is such a communication technology which already exists and which is being more and more adapted by equipment manufactures.

While today's factory automation is organized in a strictly hierarchical and pyramidal structure, the introduction of distributed control and context sensitivity will lead from the automation pyramid to the factory internet. The

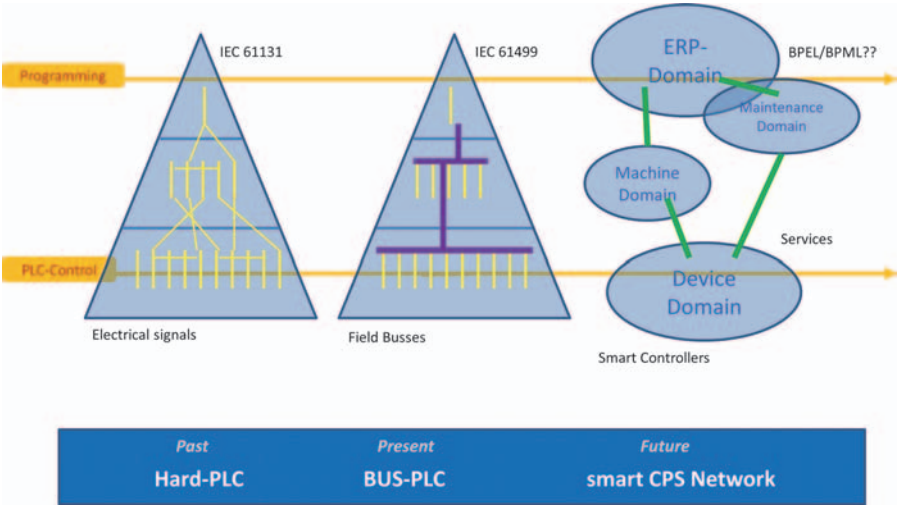

Fig. 3.6 From the automation pyramid to an automation network.

strong hierarchical control and communication structures will disappear (Figure 3.6). One of the main reasons for today's hierarchical structure has been the real time constraint for the past decades. Automated processes typically require the reaction to events within a few milliseconds. Therefore specialized automation networks have been set up not being compatible to the standard TCP/IP protocol. Here, the central logic controller of an automated production line acts as information gateway by aggregating the various signals to performance indicators and offering them to the upper layers of the pyramid. However today it is foreseeable that future revisions of the TCP/IP standard will offer better real time support. Real time behavior will evolve to a quality of service aspect enabling the realization of real time enabled subnets and offering the addressability of every network partner [7].

3.3.3.3 The augmented operator

The utilization of the smart product, equipment and infrastructure will lead to a huge amount of available data. The human will need to access situation dependent filter mechanisms in order to decode the data noise. Context information such as the task, the role or the intention of the human as well as

the location, product status or costumer information can help to identify the situation and to configure the filter mechanisms.

While the consumer world already takes advantage of context sensitive applications, industrial applications are still missing. In contrast to the consumer world the relevant context information is distributed over a large number of IT systems like enterprise resource planning, plant data collection or product lifecycle management systems and even sensor systems e.g., to localize the human operator. The key to the realization of context sensitive data tailoring is the effective implementation of data krakens interfacing all the different systems and extracting the relevant context information. The context sensitive assistance requires the integrated access to every layer of the company and so requires the existence of a nonhierarchical factory internet.

From the point of view of the human machine interface augmented reality interfaces offer a lot of potential. Notably tablet computers with integrated cameras, high computing power and the capability to wireless networking are very well suited to implement such applications. The camera can be used to identify objects; the networking capability enables the access of various content data bases and the high computing power enables the superposition of the identified context to the real image. A SmartFactory^{KL} survey showed that about 78% of the participants can imagine the utilization of augmented reality in the context of factory automation. Major application fields are maintenance, logistics and training [8].

3.3.4 Lessons Learned

The mentioned technology concepts have been implemented by a number of SmartFactory^{KL} partners from industry within public and private projects. The following conclusions reflect the experience gained in those projects since the founding of the technology initiative in 2004.

From the pure technological point of view huge advances have been made in recent years. Auto ID technologies, Wireless communication standards and Ethernet based field busses have reached a high level of maturity. With well accepted standards like OPC-UA, specifications and reference implementations of non realtime M2M communication are being developed. Field devices as well as MES and ERP software systems implementing OPC-UA are offered.

So in terms of networks and addressability of factory components basic IoT technology is available.

IoT applications often base on the content generated within the complete lifecycle of products as well as equipment. Bringing IoT applications to life means to solve the digital factory dilemma first. I.e., make PLM tools interoperable, make information from various CAx systems analyzable and bridge the gap between product development and manufacturing. In today's companies typically various engineering tools are used. The reuse of the generated models is limited due to incompatible data formats and implicit modeling prerequisites. Here the application of semantic meta models is a promising technological approach. However, there is a huge organizational issue in the cooperation of functional entities in today's companies.

Introducing the IoT in factories means to make information streams lean. While the stream of material and products through the plant has been subject to optimization for quite a long time, the meaning of information and knowledge streams is not yet in the focus of production engineers. Analyzing information and knowledge streams in today's factories is neither a core competence of automation nor of production engineers. We need experts and methods to focus the knowledge and information streams. Applied informatics has to enter our companies focusing the instantiation of methods and algorithms.

If the basic technology is available then implementing IoT applications is a matter of specification and integration. The specification of such processes and services is a creative act and requires both technological competence and domain knowledge in the application field. The relation between IoT technology and application relevant performance indicators (i.e. more turnover, better product quality, etc.) is neither trivial nor self-explaining. Not the technology itself but the use of technology yields to better processes and in turn to a benefit. Experts in both domains are very rare.

Here, one of the core issues realizing IoT applications seems to reside. Compared to purely technology oriented projects, the number of application projects within SmartFactory^{KL} is small.

Finally, as those lessons learned show, introducing the IoT to the factory has a deep impact on factory processes not only on a technological but also on an organizational level. In order to get the most out of this ongoing change, primarily experts and methods are needed to assess the benefit of new processes and added value services based on the abundant availability of information.

3.4 Brownfield IoT: Technologies for Retrofitting

The Internet of Things aims to be a disruptive technology in many ways and may change how future industry will work. However, enabling technologies like RFID or Wireless Sensor Networks are in place, it is often hindered by the fact that huge investments are needed and the local value is considered too low for adoption. The creation of a global network of various ubiquitous networks is one of the driving technological vision behind the Internet of Things. The economical vision of creating domain-and network-wide business fields and usage scenarios by pervasive information networking uses the "Internet" both as a technical and economical analogon. On one hand, as the global IP-based network that connects over 5 billion devices of different networks, and on the other the resulting economic growth and business cases. The interesting fact is, however, that a lot of the enabling technology of the Internet of Things is made to work in a very resource efficient way that hinders such efforts. Novel applications are often enabled only by proprietary technology that uses local optimizations and does not primarily consider inter-networking aspects.

Industrial infrastructures are often older that the networks that formed the initial Internet. They can by no means be considered a green field, but consists of a large installed base with machinery that has lifetimes of up to 40 years. Thus many of the applications of IoT technology (as depicted in Figure 3.7) that we consider to have high potential value involve retrofitting

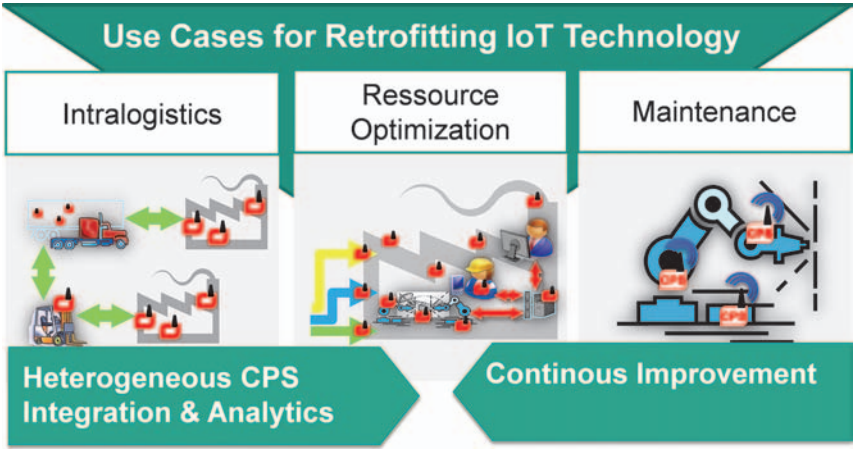

Fig. 3.7 High value use cases for IoT retrofitting.

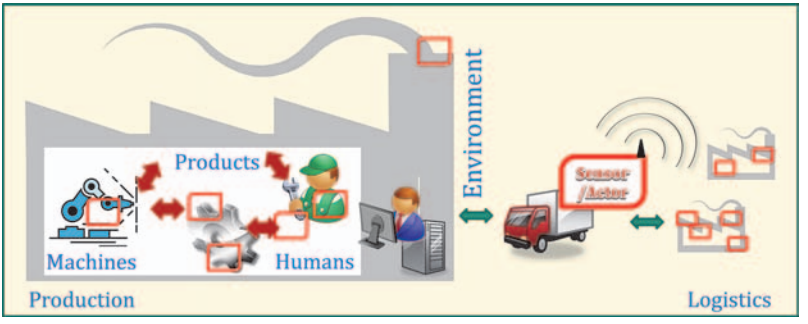

Fig. 3.8 Iot supported interactions as part of a complex Cyber-Physical-System.

industrial systems with IoT systems. These "brownfield" use cases are all targeted towards optimizing existing processes by decreasing the gap between the real world and the virtual world. They are thus examples for an evolutionary approach towards an "Industry 4.0" that builds upon IoT Technology.

As depicted in Figure 3.8 so called cyber-physical-systems in an industrial environment are by definition heavily interconnected. They reflect their physical interdependencies also by communication link and data exchange. Technologies like sensor networks and RFID often builds the missing link in such an environment. IoT technology delivers "smartness" and context awareness to otherwise "dumb" objects and environments. It puts the human in the loop of many otherwise ad-hoc and unstructured business processes.

As a motivating example of a very simple use case for such a system we consider a mobile maintenance use case. In such a scenario a service technician comes onto the site of a client and can identify all machinery parts easily using RFID and ad-hoc device discovery. Based on this information he can build an up-to-date image of the current system state that can be augmented with historical and semantically interconnected data. He can further deploy wireless measurement devices ad-hoc to gather missing parameters to guide his diagnosis and maintenance strategy. Such an ad-hoc setting is an example for the integration of federated heterogeneous sensor information as core of an informed maintenance strategy with high immediate value coming from IoT technology beyond high infrastructural investments [11].

3.4.1 Cost-effective Technical Integration of IoT Devices

A developer of IoT technology has to take various technical requirements into account such as energy, communication bandwidth, communication topology

or processing resources of different IoT systems. Additionally the interoperability is crucial to the value of the system. Assuming that in the future the service technician interconnects with a whole range of different types of wireless measurement systems and smart machines of different manufacturers, the analysis application must be aware of the semantics of all interfaces. Furthermore, the ability of the system which consists of heterogeneous components to integrate in the field, to configure and calibrate crucial for the application of ad-hoc networked sensor system in the maintenance scenario. Loosely coupled, document-based Web services provide a well-defined path to configuration and measurement data from wireless ad hoc systems and automation systems, however, have the disadvantage of a very high runtime overhead.

First, standardized ways must be found to obtain comparable quality data sets with opportunistic, distributed measurements. In addition to the demands on the sensor also just coming aspects of this case are concerned. In distributed measurements, such as fine-grained synchronization of distributed measurements of importance, and therefore optimized MAC protocols are required. Second, a live data acquisition, needs a high throughput of data (eg $\sim$, 2 kHz $*$ 3 channels $\times$ 16 bits $=$ 96 kbps) to ensure that, while energy efficiency of the hardware, requires a high efficiency of bandwidth usage. The IEEE 802.15.4–2006 2.4 GHz PHY supports ideally a fixed channel data rate of 250 kbps with a maximum payload data rate of approximately 101 kbps. Without optimization, the sensing and transmission of a three-axis acceleration value is simply not feasible at 1 kHz bandwidth. Therefore many vendor resort to proprietary solutions.

This also explains why, despite increased standardization efforts in this area have shown only limited influence. Even on top of successful standardizations like 802.15.4 there is a fragmentation of protocols like ZigBee (Pro), or the wireless HART OPC binary protocols that address domain specific problems. This foils efforts for cross-domain applications. If we broaden the scope and think of a real Internet of Thing technologies used range from Web Services and Wireless LAN via proprietary sensor and home automation networks globally used wireless technologies such as EPC protocols for RFID applications. More diversity is introduced through a variety of programming models, tool support, operating systems, and programming languages parallelism.

Especially, data from different (ad-hoc) measurements, e.g., wireless sensing devices, need to be propagated and integrated in a reusable way, to provide a smooth propagation path of data from on-site mobile data collection towards

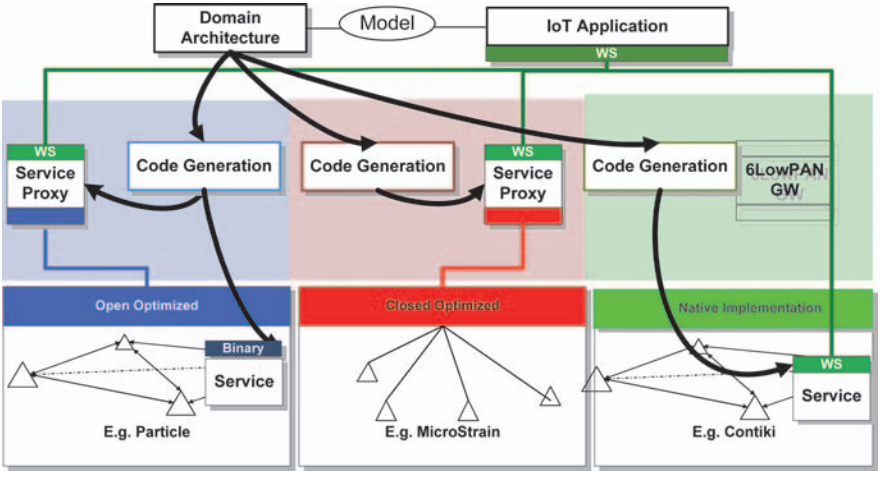

Fig. 3.9 TECO-Generated gateway architecture for exposing IoT to an ad-hoc SOA.

enterprise data management. Mature exchange formats for time series and transient recording in the field already address the problem of describing the measurement conditions. While the time series data is a structured format, the measurement description and the configuration file which are essential for understanding and analyzing the data at a later stage, are not often available in a machine-readable and semantically self-descriptive form. Building on top of this philosophy, for example, loosely-coupled structured message-based web-services provide a well-defined way to exchange configuration and measurement data with sensor nodes and automation systems [12, 13].

We have developed pragmatic light-weight strategies [12] for combining on-site online (real-time) measurement and configuration services with post-measurement enterprise data-exchange in a consistent way by using web services and model-based data transfers down to device level. In general, wireless ad-hoc measurements highly depend on the measurement context. By building on ideas presented in [14] we can provide a contextual framework for federating this information (with respect to context parameters such as: location, time, causal relation to configuration and setup, measured equipment, sensor, device capabilities). We describe aspects specific to field measurement and maintenance tasks in semantically linked way and the framework will directly integrate existing workflows with a mobile ad-hoc measurement setup on-site. In contrast to common existing approaches we especially trade-off between

complexity and practicability of data gathering in terms of overall cost for implementation by work practices and in terms of overall cost for adoption of third-party vendors (typically problem-focused SMEs).

To lower the cost for developing services, protocol translators and gateways we heavily employed model driven development tools. Considering the consistency and tool support for data meta-models we decided to use the EMOF (ISO/IEC 19502:2005). We use subset of EMOF as our intermediate representation for generating service that is also known as the class of regular nested word languages. Their properties make it particularly suitable for representing XML structures and for supporting modular design of protocol translators on networked embedded devices. On this basis we have developed a model-driven work flow within the Eclipse Modelling Framework for developing message translation for IoT subsystems [12] that largely automates the process of developing gateway system as well as message binding for the IoT platform. With this system we are able to quickly adapt multiple standard and proprietary platforms to service oriented architecture that seamlessly integrates into the existing IT landscape and enable new forms of human machine interaction like ad-hoc sensor augmented reality for maintenance [15].

3.4.2 Cost-effective Process Integration of IoT Devices

Not only the integration but also the IoT enabled processes needs to be cost-effective by design and well integrated. Our approach is evolving around existing processes and scaling with the human information consumer, rather than solely relying on big data analytics and total connectivity.

1. Opportunistic data collection through local infrastructures and ad-hoc mobile access
2. Context-aware interlinking of heterogeneous data starting from existing processes
3. Human agility and expertise supported by a human-centered information design

Global interoperability in contrast to global connectivity and the use of mobile devices can enable the user to access IoT services ad-hoc. Users are informed in-situ by distributed sensing system, heterogeneous linked data sources and social media paradigms. Building a sensing enterprise from

existing technology will require a considerable jump forward in terms of sensing system deployment and configuration, reasoning on linked data, human-computer interaction and adaptable work flows. New approaches are needed for context-aware annotation, synchronization, visualization and triggers on local and remote data.

Current studies have shown that huge saving potentials in existing processes are targeting the work of engineers on site. There is still a potential of 10–40% for making work more efficient and an even higher saving potential (10–50%) from relieving the workload [15, 16]. With more information sources at hand, the overall efficiency may increase in the long run. However, the additional responsibility of collecting and documenting fine granular lifecycle information may add extra responsibilities to each worker, thus increasing the workload.

In the backend, new intelligent methods based on semantic technologies and tools for processing and analyzing historical and on-site data are still necessary to deal with the different qualities of data. Indeed, collection, retrieval and analysis of real- and life-time data need to be seamlessly integrated into real service and design processes without producing unnecessary (cognitive) overhead for the human engineer on and off-site. In conclusion, a combination of integrated technologies is expected to offer new methods, tools and applications to create market opportunities in terms of new services, new methods and software. New business models that support and enhance cooperative networking among the enterprise assets and artifacts are expected to arise.

One of the earliest work in this direction was done in the EU FP6 CoBIs Project (http://www.cobis-online.de) Work with relation to proactive user support for unstructured tasks considering processes and real-time information was also researched in the ADiWa project (http://www.adiwa.net), funded by the BMBF (German Federal Ministry of Education and Research) or European projects like makeSense. The makeSense (http://www.project-makesense.eu) research project is focuses on modeling business processes where a subset is compiled into executable code that is directly executed by a Wireless Sensor Network. As enterprise data is usually very long-living and of continuous value, but CPS need to frequently adopt and reflect changes in the production evolution, the FP7 Timbus project (http://timbusproject.net/) is looking at timeless context-aware business processes and supports the long-term continued access also to IoT generated data and underlying dynamic analysis infrastructures.

3.5 Smart Objects, Smart Applications

In the Vision of an Internet of Things interconnected Smart Objects play an important role. Such a Smart Object is a bi-directional communicating object which observes its environment and is able to make decisions depending on the application and based on the information extracted from the physical world.

One approach to Smart Objects is based on the technology of wireless sensor networks, as they already provide the communication platform and the sensors.

The ISO/IEC JTC1/WG7 Working Group on Sensor Networks has designed reference architecture Figure 3.10, which separates the sensor node functionality into three layers:

- Communication as part of the basic functions layer: describes the communication protocol for the interaction of a smart object with other smart objects, an infrastructure or backbone networks.
- Service Layer: represents a set of functions commonly required, such as sensor information gathering, filtering by various policies and rules, data comparison and analysis, data mining, context modeling, context-aware processing, self-localization, context-aware decision and estimation.
- Application Layer: realizes the use case of a smart object by a set of functions to users to meet defined requirements.

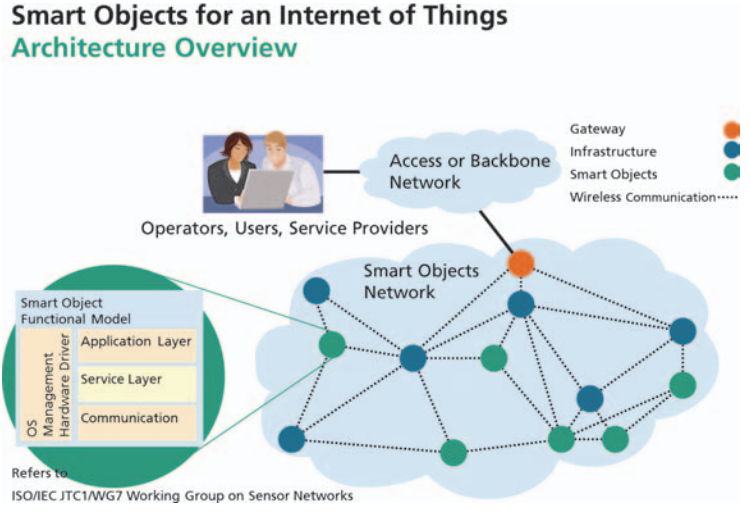

Fig. 3.10 Architecture overview of interconnected smart objects.

From the users prospect the smartness of a smart object is realized within the service and the application layers. Additional value can be achieved through generic, reconfigurable Smart Objects. They offer a set of services and functions for a specific application domain and are adapted to project or user requirements by reconfiguration by a user or a service provider.

Smart objects are designed as miniaturized, low power microelectronic systems based on micro controllers, transceivers, sensors and energy supply.

As these microelectronic systems provide very limited resources (i.e., processing power, memory) reconfigurable software implementations for smart objects become a challenge, especially when reconfiguration should be possible by a user without code programming (requires easy programming) or if reconfiguration should be done over the air (requires minimum code size).

In common service oriented approaches a plurality of service components are defined. Figure 3.10 shows some components for an asset tracking application. The software interfaces of such components are well defined and communication is typically handled by a service manager in a message oriented way.

Reconfiguration is done by adding or changing components or by changing the functionality behind the interfaces. This is done by code programming of the components and by software update on the smart object.

Code Programming and data-intensive software update can be avoided by the new approach of smart applications.

Like in the service oriented approach smart applications consist of software components. In addition the components are supplemented by rule based processing and interfaces. Each component has its own rules set and parameters. The rules processing engines are able to handle events, such as messages, interrupts and synchronization.

For the definition of rule sets for the application modules a universal configuration language SAL (smart application language) has been developed at Fraunhofer IIS. The main goal of this language is, to describe instruction cycles which are triggered by incoming events. On the one hand the instructions can have executive characteristics on the other hand they can act as conditions in if-else constructs. These instructions handle two parameters, which are defined as variables of well-known data types and can be modified at runtime.

The smart application technology allows the definition of multiple rule sets for a smart object. Thus, it is possible to configure multiple application modules and interconnect them by logical links. Smart applications can be realized within a node or even distributed over a whole sensor network.

In order to make the implementation of smart applications easier for the user, a graphical development environment allows defining rule sets with the help of jigsaw puzzle pieces Figure 3.11. The editor provides SAL elements — such as events, instructions, variables and common language components — which can be connected to a jigsaw puzzle. The backend generates the corresponding SAL code and the user level is arranged on a higher abstraction layer. The following Figure 3.12 shows the complete workflow of the smart application development.

The SAL source code, generated by the graphical editor, is compiled to an optimized and highly compressed byte code. Due to the small size of the resulting data, a complete configuration can be sent via the radio interface of the smart object. It is also possible to send multiple of these configuration sets and store them on a persistent memory as application profiles and switch between them on demand.

After receiving a configuration, the smart application manager configures all corresponding modules on the node regarding to the rules. It starts the components in sequence of their application priority. The application is then ready to operate. A reconfiguration can be done at any time and with any

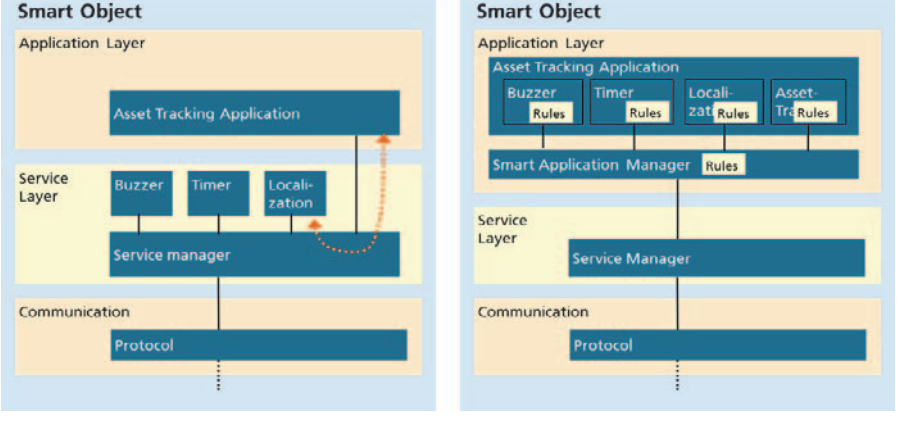

Fig. 3.11 Service oriented approach — left and Smart application approach — right.

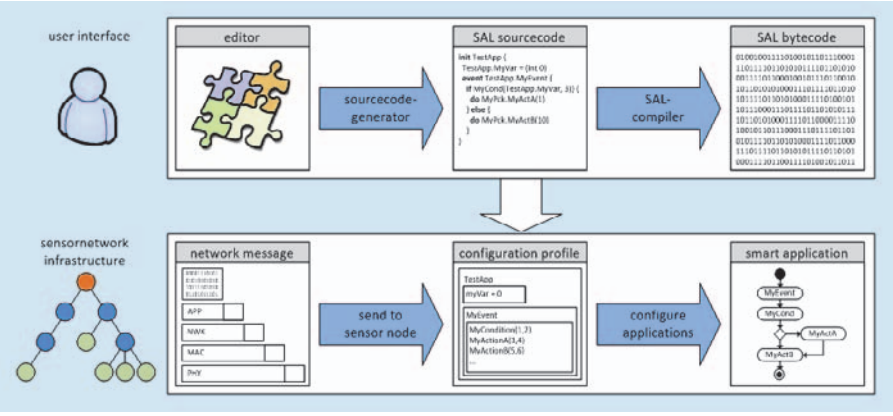

Fig. 3.12 Smart applications workflow — from a jigsaw puzzle to the application on the node.

configuration profile. The node can also be configured with a standard profile, which is loaded at the boot process of the system.

In summary the smart application approach allows changing application functionality by changing the rules of interconnected rules engines in the service components. This can easily be done by a graphical puzzle editor. The generated smart application language code is very compact and allows very efficient reprogramming of all or selected nodes over the air.

The smart application approach is an ideal solution for adapting generic smart objects to different projects or use cases in the same application domain.

3.6 Four Aspects in your Business to Master IoT

3.6.1 Internet Conquering Product Business

In order to deliver value for business it is too narrow to just look at connectivity. It is important to look at the business process and the benefit for the involved stakeholders in a specific application.

In recent years, the internet has transformed communications (Voice over IP, Twitter), the media landscape (news, advertising), commerce (eBay, Amazon) and the music industry (file sharing, online music stores). Now, smartphones and tablets are helping it to permeate our professional and private

lives. Given that daily life is ever more interactive and networked, and our contacts ever more global, I increasingly expect everyday objects to be more intelligent and networked, too.

The Internet of Things (IoT) is the next generation of the internet. It is a global system of interconnected computer networks, sensors, actuators, and devices that use the internet protocol to potentially connect every physical object. By merging this physical world with software from the virtual world, organizations, companies, and consumers will benefit from new services that emerge from web-based business models. In the final analysis, however, IoT stands for the start of a series of technological and above all economic changes that will revolutionize not only the marketplace as we know it but also the lives of each and every one of us.

The Internet of Things & Services is merging the physical and virtual world. Impressive is the growth that is seen in internet access. Whereas in 1995, less than 1% of the world's population was online, this number has exploded: 2.3 billion people were online in 2011, while for the year 2015 we expect 5.5 billion people to have internet access (source: ITU). This equates to around 75% of the world's population, Figure 3.13. Expected devices connected to internet have been estimated by Bosch Software Innovations, to 6.593 billion by 2015, Figure 3.14.

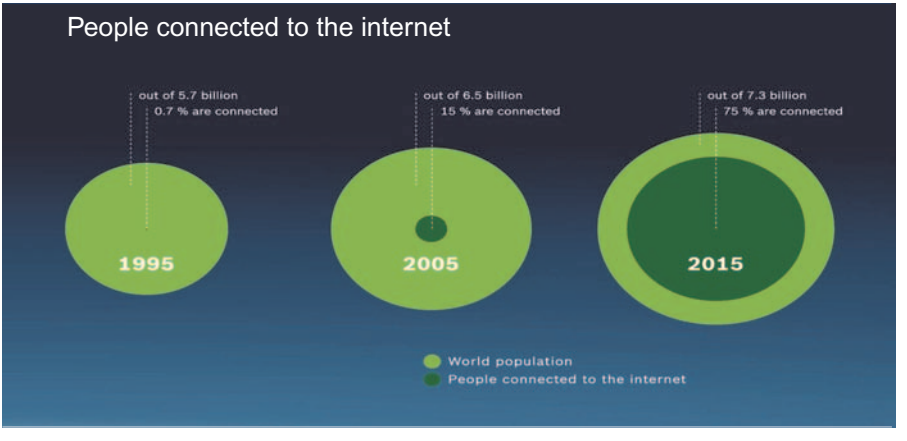

Fig. 3.13 Impressive is the growth that is seen in internet access.

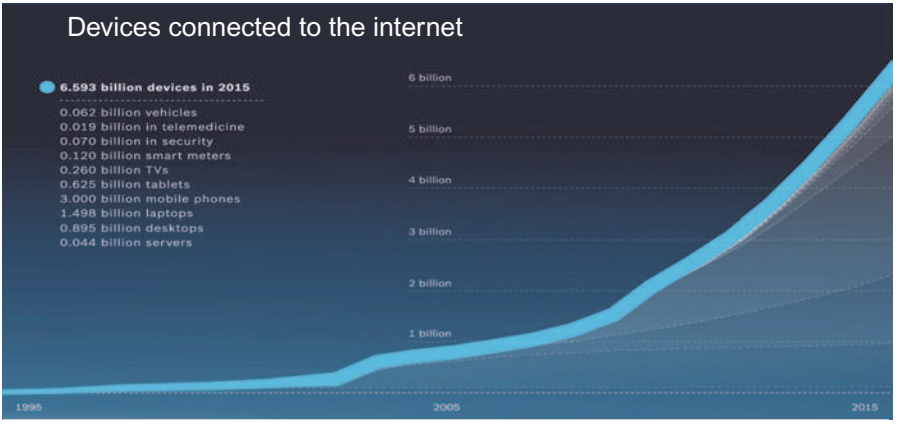

Fig. 3.14 By 2015 expected IP-ready devices, connected to the internet, 6,593 billion.

3.6.2 Strategic Business Aspects

For us the Internet of Things & Services, Web 3.0, m2m, or cyber physical systems are much more than just buzzwords for the outlook of connecting more than 6 billion devices by 2015. It is a chance and a challenge to bring the internet and physical world closer to each other. We understand the Internet of Things & Services along four dimensions:

Four Aspects of the Internet of Things & Services

- Technology: The internet and its technology are vivid drivers offering an established platform for interconnecting billion things — from tiny sensors, smart phones, PCs, to high performance computers. Open Source communities scale and accelerate the technology development and the implementation of open standards. Therefore, business moves to system and software platforms in the internet.
- Business Innovation: Weaving smart things, enterprises, and people leads to innovation in services and business models. The spirit of internet business models is turning up in traditional product business (e.g., pay-per-use for car sharing).
- Market: Different industries meet the first time as the Internet of Things & Services crosscuts some of today's separate markets (e.g., Electric Vehicle Roaming with Energy and Mobility companies). The players of these markets compete and cooperate in

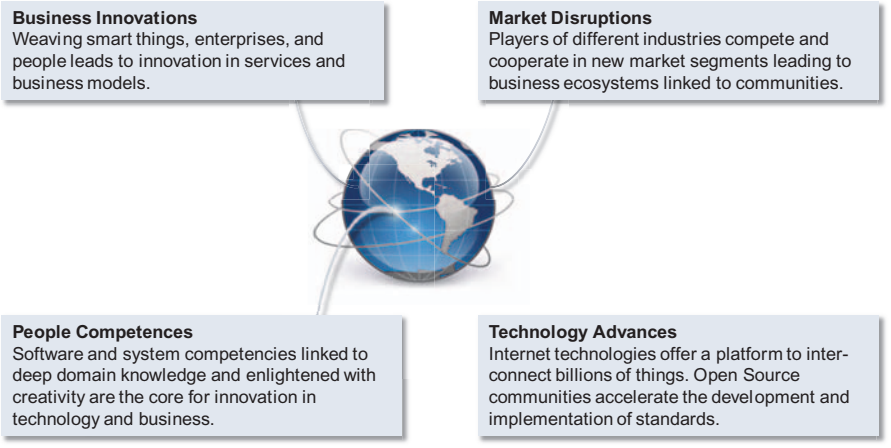
Business Innovations
Weaving smart things, enterprises, and people leads to innovation in services and business models.
Market Disruptions
Players of different industries compete and cooperate in new market segments leading to business ecosystems linked to communities.
People Competences
Software and system competencies linked to deep domain knowledge and enlightened with creativity are the core for innovation in technology and business.
Technology Advances
Internet technologies offer a platform to interconnect billions of things. Open Source communities accelerate the development and implementation of standards.

Fig. 3.15 Internet of Things & Services four dimensions.

new segments leading to business ecosystems that are linked to social communities (e.g., Google+) and open source communities (e.g., Eclipse).

- Competencies: Software and system competencies linked to deep domain knowledge and enlightened with creativity are the core for innovation in technology and business.

3.6.3 Vertical Business Domains for IoT

The value of the Internet of Things & Services technology is delivered in vertical application domains. There are many hot candidates to be early movers such as connected energy and connected industry.

3.6.3.1 Connected energy

We are currently witnessing a paradigm shift in today's energy market. From the dogma of a production structure with large power plants to a world of many small, distributed power generation systems. Low voltage networks are especially affected by these changes and are facing new challenges. Today, the many distributed power generation systems are connected to the low voltage grid, but not transparently. Consequently, distribution grid operators are forced to react instead of being able to act in order to ensure network stability.

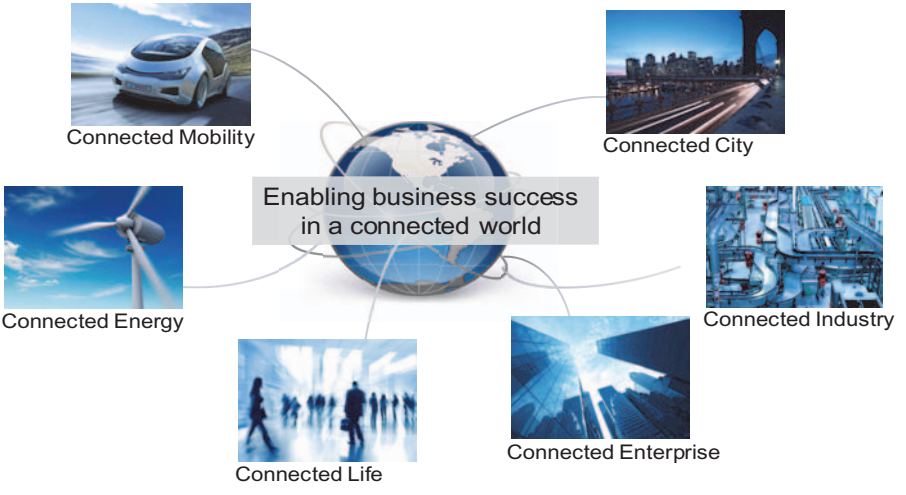

Fig. 3.16 Applications for the Internet of Things & Services.

While large power plants operate based on accurate and agile schedules, decentralized power generation plants are often operated along subsidy policies and not according to the forces of the electricity market. This leads to an uncontrollable volatility in production and highly fluctuating market prices. It also forces transmission and distribution network operators to maintain high balance energy capacities in order to ensure grid stability.

Aiming for a better integration of distributed power generation systems, regulations are changing, and with it the demand for intelligent energy management systems is increasing. Their purpose is to provide for a transparent integration and control of distributed systems to improve the efficiency of sub-systems (e.g., a microgrid) in the smart grid as well as to give both new and established market players the opportunity to profit from new market potentials.

The virtual power plant is an example of how the operation of such a sub-system can already be profitable based on Internet of Things & Services technology. The service is supposed to help implement new business models, not only for traditional market players such as local energy producers, traders, aggregators and operators, but also for large companies and industrial parks. They could use the service to make profit, e.g., by offering spare capacities of unused facilities.

3.6.3.2 Connected industry

The Internet of Things in production and logistics is coined with the term "Industrie 4.0" in Germany. Industrie 4.0 is paving the way for a social and technological revolution that will drastically change the entire industrial landscape. Why 4.0? As since the 18th century, when the first Industrial Revolution began, it is the fourth wave of major technological changes. Industry 4.0 is a sophisticated approach changing the entire global value chain: communication, planning, logistics and production.

The German industry, academia, associations, and unions compiled a report on how this transformation can be achieved:

> *"Industrie 4.0 holds huge potential. Smart factories allow individual customer requirements to be met and mean that even one-off items can be manufactured profitably. In Industrie 4.0, dynamic business and engineering processes enable last-minute changes to production and deliver the ability to respond flexibly to disruptions and failures on behalf of suppliers, for example. End-to-end transparency is provided over the manufacturing process, facilitating optimised decision-making. Industrie 4.0 will also result in new ways of creating value and novel business models. In particular, it will provide start-ups and small businesses with the opportunity to develop and provide downstream services. In addition, Industrie 4.0 will address and solve some of the challenges facing the world today such as resource and energy efficiency, urban production and demographic change. Industrie 4.0 enables continuous resource productivity and efficiency gains to be delivered across the entire value network. It allows work to be organised in a way that takes demographic change and social factors into account. Smart assistance systems release workers from having to perform routine tasks, enabling them to focus on creative, value-added activities. In view of the impending shortage of skilled workers, this will allow older workers to extend their working lives and remain productive for longer. Flexible work organisation will enable worker to combine their work, private lives and continuing professional*

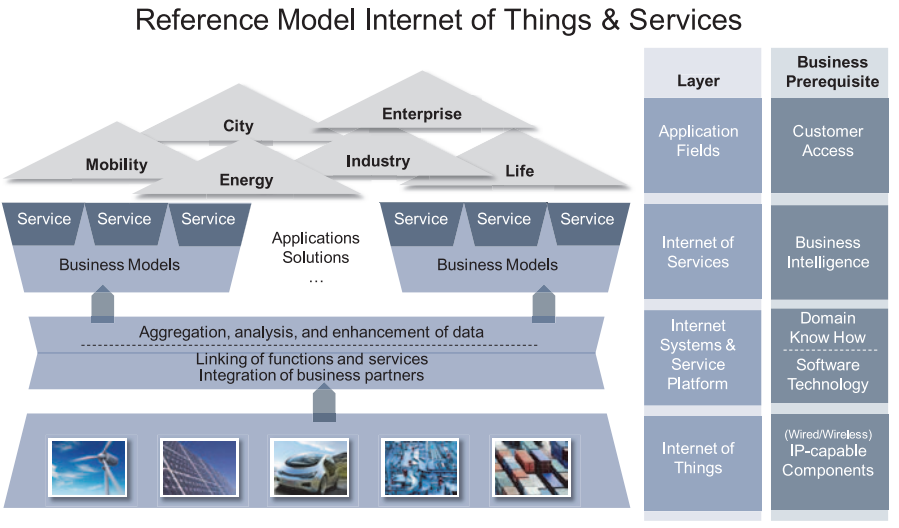

Fig. 3.17 Bosch Software Innovations reference model for the Internet of Things & Services.

> *development more effectively, promoting a better work-life balance."*

[source: acatech 2013] The national academy of Science and Engineering (acatech): Recommendations for implementing the strategic initiative INDUSTRIE 4.0, April 2013 Securing the future of German manufacturing industry, Final report of the Industrie 4.0 Working Group.

3.6.4 Reference Architecture and the Core Competence for Business

The business success in one vertical domain is the key entry point, but successful architectures will reach out to other verticals later. Only architectures that can cover multiple domains will be successful in the long run, as the domain "silos" of the past still prevents a lot of innovation between the domains: e.g., between automotive and energy in electromobility.

3.7 Auto_ID — Value Creation from Big Data and Serialization in the Pharmaceutical Industry

Industries are maturing at a faster rate than ever before — manufacturing is increasingly distributed and outsourced — and where costs have been taken out

of production systems through initiatives such as Lean Production [18 Womak, 1990], companies are increasingly looking to optimize savings across the total product lifecycle. This chapter explores IoT technology as a value creation capability rather than as a cost optimization strategy, specifically exploring the value of data that is collected from multiple infrastructures across a product lifecycle and where the Auto-ID serialized identifier may serve as a key to linking relevant data to individual products, processes and related outcomes. Ultimately the hope would be that data from anywhere in the product lifecycle might facilitate the development, trials and approvals of New Chemical Entities (NCEs) and New Biological Entities (NBEs).

3.7.1 Background — Serialization Role in an 'Internet of Things'

As industries instrument complex processes beyond manufacturing plants in the supply chain and aftermarket services, Automated Information Data Collection (AIDC) technologies including optical scanning of printed linear or 2D bar codes, radio frequency "reads" of passive RFID tags together with new telemetry technologies, provide a powerful portfolio of tools for product lifecycle visibility. Whether sensors are connected in an 'Internet of Things' via M2M protocols, via Enterprise applications or via the Cloud [19 Auto-ID "Cloud of Things"], leveraging AIDC standards is important to making data accessible for value creation.

Serialized identifiers are the keys to building an Internet of Things; just as unique IP addresses are integral to the web itself. One global system of such identifiers, the MIT Auto-ID Center Electronic Product Code (EPC), was licensed by GS1 for use by its member manufacturers in all 124 countries, together with EPCGenII RFID specs, are now instantiated in ISO Automatic Identification and Data Capture Techniques [20ISO18000-6c]. The GS1 serialized Global Trade Identification Number (sGTIN) is being used for monitoring — a single Item Class in a 96 bit tag supports up to 200Billion #'s. Examples of serialization initiatives from this researcher's experience include part-marking schemes for aero-defence, automotive and high tech where up to 80% parts communality is shared between competitors, to tracking tobacco sales tax compliance using INTERPOL Global Register [21 IGR] or EPCGenII serialized RFID tags [22NXP, Quanray] for authenticating 100 m^+ alcoholic beverages in China and the UPU Global Mail Quality tracking system (10,000 readers in 50 countries).

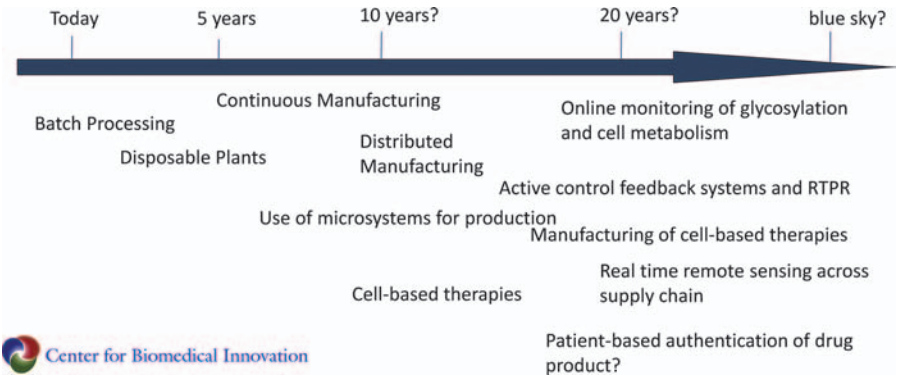

Fig. 3.18 MIT CBI BIOMAN biomanufacturing technology roadmap [31].

3.7.1.1 Big data in the pharmaceutical industry

A radical transformation of the pharmaceutical manufacturing industry is taking place, much as occurred previously in the textile and electronics manufacturing sectors. According to the FDA, imports from China to the US are expanding at a rapid pace, from 8 m shipments in 2002 to 28 m in 2012, and are expected to grow to 34 m in 2013. In fiscal year 2011, more than two million lines of FDA-regulated products were presented for entry into the United States from China. Simultaneously with the growth in data from normal supply chain processes, an industry transition to distributed, disposable and continuous manufacturing processes as foreseen in the MIT Center for Biomedical Innovation BIOMAN consortium roadmap promises explosive growth of Big Data in this industry.

Big Data can be compared to the discovery of the microscope, Professor Eric Byrnolfsson, Ph.D. said in his keynote at the MIT Sloan "Big Data: The Management Revolution" conference and in a recent Harvard Business Review article [23 Brynolfsson, 2012]. Big data holds huge, largely untapped potential to change the way healthcare functions as an industry. MIT is studying it in a five year US$ 12 million partnership [24 BigData@CSAIL] with Intel to explore techniques for organizing and making sense of the huge amounts of information generated by Web users and networked sensors.

Furthermore data from the 'last mile' of the supply chain such as the ability to track product and the data associated with patient interactions and outcomes as recorded in the electronic Health Record (eHR) has eluded the industry until

now. The biologics industry has been a pioneer in re-establishing data linkages between pharmaceutical manufacturers and clinical service providers in the context of developing stratified medicine and autologous cell based therapies which require matching the right cells with the right patients.

We can see this linkage of product and patient outcomes at the center of the "7 Flows" model proposed by Genzyme executive Laurent Boer, VP Global Distribution & Logistics and General Manager of the Genzyme Northborough Operations Center, as a framework to think about the kinds of data that are required for managing pharmaceutical industry processes [25 Boer, 2013].

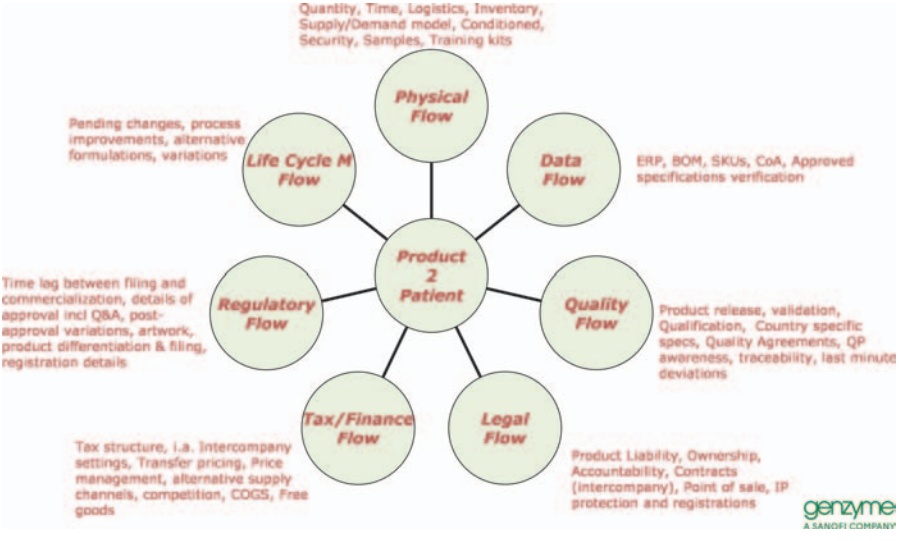
Quantity, Time, Logistics, Inventory, Supply/Demand model, Conditioned, Security, Samples, Training kits
Physical Flow
Pending changes, process improvements, alternative formulations, variations
Life Cycle M Flow
Data Flow
ERP, BOM, SKUs, CoA, Approved specifications verification
Product 2 Patient
Time lag between filing and commercialization, details of approval incl Q&A, post-approval variations, artwork, product differentiation & filing, registration details
Regulatory Flow
Quality Flow
Product release, validation, Qualification, Country specific specs, Quality Agreements, QP awareness, traceability, last minute deviations
Tax/Finance Flow
Legal Flow
Tax structure, i.a. Intercompany settings, Transfer pricing, Price management, alternative supply channels, competition, COGS, Free goods
Product Liability, Ownership, Accountability, Contracts (intercompany), Point of sale, IP protection and registrations
genzyme
A SANOFI COMPANY

Fig. 3.19 The 7 flows of supply chain information — Laurent Boer, VP global distribution & logistics, Genzyme — Sanofi [32].

In the following section we will review these (7) data protocols. The connection between a product and a patient outcome is an area of great promise for pharmaceutical manufacturers developing stratified medicine therapeutics.

3.7.1.2 Tracking serialized products

In the healthcare industry there is no question that both regulatory agencies and pharmaceutical product manufacturers would be better off with identification systems for tracking products, producers, production sites as well as individual

patients and associated product-patient outcomes in order to optimize the development and distribution of cost effective and quality therapeutics. The industry is already making significant investments, in response to regulatory mandates from countries including Argentina, China, Turkey and the State of California, to modify production-labelling systems to support serialization.

In the first phase of implementing serialization the pharmaceutical industry is adopting 2D optical bar code as a transport and the GS-1 serialized Global Trade identification Number (sGTIN) symbology. In tracking physical goods there is some debate about whether e-Pedigree specifications should include a requirement for tracking the aggregation/disaggregation of each item as it moves across the supply chain — adding expense to the process. One industry expert cites the difference in some businesses as a cost differential between $20,000 per manufacturing line and $200,000 per line for the manufacturer. The distributor/retailers however support tracking aggregation so that they can ship and receive items at a higher shipping hierarchy, i.e. pallets versus cases, or cases versus "eaches" in the supply chain, since reading 2D barcodes on conveyors running at speeds of 200+ crates per minute will be difficult. Further research and guidance from regulators is required to ensure tracking systems interoperability.

3.7.1.3 The value of supply chain data

Product identifiers on a label can serve as a "key" to information about the processes and conditions through which the product has travelled. Once product label serialization is implemented, as in the case of recent deployments by apparel companies including Macy's and American Apparel, the first question these organizations must address is, as Joseph Andraski, President of Voluntary Interindustry Commerce Solutions Association (VICS) ecommerce Standards Data Organization (SDO) has been asking is, "What to do with the data?"

One answer is that the pharmaceutical industry would clearly benefit from knowing "who" is making "what"; "where" products are being manufactured; under what conditions they are being produced; and how the aforementioned factors interplay with these elements to lower commercial friction or, by contrast, to create elevated risk in the manufacturing and supply chain.

One example of the value that can be derived from serialization was presented in a keynote by AbhiDhar, CIO of the eCommerce division,

Walgreens, at the Auto-ID Labs 2012 Big Data Conference [26Auto-ID Big Data] organized with GS-1 and VICS: the use of the serialized identifier for prescription refills. For Walgreens today, the majority of web orders for refills are now placed by consumers using a smartphone barcode scanning application that 'reads' the 2D barcode on the pill-box label which the system uses to look up the initial order which is to be refilled. As we can see from this example, Big Data, when tied to individually identified products and/or transactions, allows a company to link data captured in the physical world or somewhere on the web, to Enterprise systems processes.

3.7.1.4 Quality by design

The cornerstone of FDA's quality initiative, Pharmaceutical CGMPs for the 21st Century — A Risked Based Regulatory Approach — takes a Process Analytic Technology (PAT) and Quality be Design (QbD) holistic approach to identifying sources of variability (in raw materials, in-process materials and process factors), to managing variability through process understanding and risk-mitigating control strategies to improve productivity and product quality throughout the product lifecycle. Underlying this approach is the notion that quality should be built-in (i.e., by design).

Harmonization achievements in the Quality area include milestones such as the conduct of stability studies, defining relevant thresholds for impurities testing and a more flexible approach to pharmaceutical quality based on Good Manufacturing Practice (GMP) risk management. Specific areas include Stability, Analytical Validation, Impurities, Pharmacopoeias, Pharmaceutical Development and the Development and Manufacture of Drug Substances. As manufacturing supply chains extend around the world, ASTM in E2500-07 and ICH in Q8 (R2), Q9 and Q10 SDO's have developed guidelines for GMP regulations for the industry.

In consortia such the MIT CBI BioMANufacturing Research Program [27 BIOMAN], academia is also working with regulators and industry sponsors to define advanced GMP, PAT and QbD processes for optimized quality manufacturing and to develop tools to assess and mitigate risk in biopharmaceutical production. One approach the group has been discussing with industry sponsors is to investigate QbD applicability to quality oversight of the global pharmaceutical supply chain.

3.7.1.5 Legal information flows

Legal issues around data exchange can be divided into two separate concerns, one is the question of jurisdiction over data, and secondly, within that context, what party(s) own the data. In the US for example, despite a common interest in ensuring efficient oversight and promoting safe and environmentally friendly products, the FDA has not been active in developing national standards on transportation and drug packaging, Unit of Use labelling and sustainability guidelines and has instead relied on local and state governments to regulate material composition, reuse, recycling, and recovery of packaging through legislation and ordinance. By contrast EU Directive 94/62/EC, "Packaging and Packaging Waste Directive" (PPWD) and the associated ISO/TC 122/SC 4, "Packaging and environment" are driving packaging changes in that jurisdiction.

Even where there are no jurisdictional issues, "who owns the data" is a challenge issue for industry stakeholders. Under current US healthcare legislation a patient has rights to access their records, but who owns this data, the doctor, the hospital, the software or hardware/services provider? Developing secure marketplace mechanisms for the exchange of patient data was the topic of one session at the PDA/FDA Pharmaceutical Supply Chain Integrity Conference [28 Miles, 2012].

3.7.1.6 Finance flows

Data is a core asset of every company and a strategic resource that can be harvested with advances in AIDC technologies. Every step in the development, clinical trials, manufacturing, distribution and service delivery of a biologics product involves massive amounts of data. Extensive industry guidelines and best practices are established for the use of this information in specific contexts such as quality control or product authentication. Good Manufacturing Practice (GMP) production and testing practices ensure quality products.

A parallel assessment of data asset values, liabilities and exchange mechanisms for these data assets is warranted in light of pharmaceutical development, technology transfer, commercial manufacturing and product discontinuation processes. The value of products as they move through the supply

chain impacts what hazards they are exposed to. For example while Viagra still is the most counterfeited product in the world today, cancer drugs now represent an increasing share of that market as reported in the Wall Street Journal.[1] It is not surprising to see that those willing to put people's lives in danger to make money see greater potential in counterfeiting a vial of Avastin that sells for $2,400, than manufacturing a $15 or $20 bottle of fake Viagra. An integrated financial risk management system is required for curating and valuing data assets.

3.7.1.7 Regulatory oversight

Automating FDA inspection/data collection processes is but one example of where changes from manual to automated data collection processes is needed. Using today's onsite inspection methodology, according to the FDA budget request to Congress in 2013, the Agency said it's inspections of foreign manufacturers jumped 10% last year to 813 inspections in 62 countries. The Agency said nearly half of the 46 warning letters issued to foreign manufacturers resulted from these inspections. What might those tallies look like if the FDA were able to inspect (200,000) pharmaceutical ingredient production sites in Asia? To quantify the size of the problem, working with FDA partner agencies International Criminal Police Organization (Interpol) and the World Health Organization (WHO), approximately 20 million pills, bottles and sachets of counterfeit and illegal medicines were seized in a five-month operation in China and nearby Asian countries in 2009 [29 WHO, 2010]. Asia has the largest amount of counterfeit medications but these illegal acts can be found worldwide. Automated mechanisms for manufacturing and supply chain compliance reporting is an area requiring further collaboration.

3.7.1.8 Product lifecycle management data

In the US healthcare market, the lack of visibility over the product lifecycle of drugs results in a $11 billion in "revenue leakage," according to a study by IDC, that could be reduced by better drug tracking [30 IDC Tech Insight, 2010]. In addition to chargeback's, reverse chargeback's, duplicate

[1] "Counterfeit Cancer Medicines Multiply;" By JEANNE WHALEN And BENOIT FAUCON; (December 31, 2012, WSJ) http://online.wsj.com/article/SB10001424127887323320404578211492452353O

chargeback's, product returns, and concealed shortages, managed care and Medicaid rebates have been a growing concern. In total, the study found that revenue leakage causes pharmaceutical companies to lose approximately 4.4% of overall revenue on an annual basis. For 2009, most forecasts predict U.S. pharmacy sales will be roughly $252 billion. That means as an industry, pharmacy manufacturers will collectively lose approximately $11 billion through channel inefficiencies. That's equivalent to total revenue for a top 20 pharmaceutical manufacturer simply disappearing each year. In light of these concerns the FDA has ranked — in order of risk of adulteration — more than 1,000 active drug ingredients. A risk based assessment and model to analyse supply chain data to address lifecycle issues may be an area that big data technologies can be useful — once enough information is collected electronically using Automated Information Data Collection (AIDC) technologies to create meaningful exploratory data.

3.7.1.9 Keeping better track of things

In each of the above scenarios we see a convergence of supply chain security, product authenticity and patient safety data and the promise that this data may be incorporated in optimal data sets to facilitate the development, trials and approvals of New Chemical Entities (NCEs) and New Biological Entities (NBEs).

In summary, as biologics industry stakeholders, including manufacturers, distributors, health service providers and regulators, invest in serialization initiatives by, equipping production lines with linear and 2Dbarcode and/or RFID labelling machinery and outfitting distribution centres, pharmacies and hospitals with RFID/2D barcode readers, this author recommends a commensurate investment in defining and collaborating with biologics industry stakeholders on where the data that is collected can most effectively be used to optimize product security, patient safety and eventually, improved patient outcomes which in turn will feed new product development for research sponsors.

3.8 What the Shopping Basket Can Tell: IoT for Retailing Industry?

The Internet of Things has become a dominant term for describing the integration of information with real-world products, items, and things. Internet

of Things is broad term comprising applications from manufacturing, smart power grids, RFID, mobile applications, track & trace, traffic monitoring, smart cities and retail. Whereas it is not completely agreed upon who coined the term of Internet of Things, there can be generally identified two streams where Internet of Things roots back to.

Firstly, there is the Internet-oriented development which aims at expanding the traditional Internet of data from computer desktop devices to mobile handsets, lower power devices, down to micro-controller devices integrated and attached physical objects and things. Accordingly, research questions are how to tailor established communication and data protocols for low-power devices with limited computing capabilities (e.g., 6 lowpan). Secondly, there is the thing-oriented development which comes from associating items and things with unique identifiers in order to relate to static descriptions and dynamic status information throughout the lifetime of things. Early developments have been based on barcode and RFID (e.g., GTIN, EPC, UID) and include architecture frameworks helping to resolve unique identifiers to database locations where the information can be stored and retrieved (e.g., ONS, EPCIS).

Either way the Internet of Things gives access about real-world processes and phenomena in real time. For instance, it offers the opportunity to integrate social media into the sales floor. This allows retailers to gain more insights into the opinions of their customers and to benefit from viral marketing, as depicted by Figure 3.20. As such, a much more fine-grain understanding of real-world processes can be obtained. Thus, processes can be optimized, decisions can be based on data, and innovative services can build upon new sources of data.

In retail where margins are low and revenues are high there has been a long tradition of introducing information systems for making processes more efficient.

About 40 years ago barcode stripes have been introduced on product items for accelerating price tagging and check-out at the register. This very same technology, originally designed to be used internally among supply-chain partners, has started to reach consumers, as they can use their mobile phones today for retrieving further information about products, such as consumer opinions or price comparison. With the advent of mobile apps from e-tailers allowing to retrieve items consumer experience in stores at cheaper prices online put a new threat retailers: retailers run into the danger of becoming the free show rooms for online retailers.

Fig. 3.20 Embedding social media on the sales floor.

Fig. 3.21 Opportunities for retail using IoT.

As this technological move is hard to stop retail has to explore new opportunities and services to offer to their clients, see Figure 3.21. Thus, using IoT retails can retrieve valuable inputs from their consumers with regards to their shopping behavior and opinion on products and adapt their offerings more

instantly to the customers' needs. Furthermore, the allowing the sharing of opinions of customers can yield a new way of establishing trust between the retailer and his clients. With these services retailers should be empowered to gather attractiveness over the electronic retailers.

3.9 IoT For Oil and Gas Industry

Internet of Things is per definition access to information everywhere. For process automation IoT can be divided into Service Applications, solutions for the mobile workforce, into wireless Field Devices utilizing different radio solutions to make information in systems and devices accessible and into long range wireless communication solutions for the Remote Monitoring of a process and a plant. In this chapter we present a wireless Field Device targeting the Oil and Gas environment. Process industry in general and Oil and Gas in particular put special requirements on field devices. Devices have to operate under harsh conditions; dirt, often high temperatures and sometimes in explosion prone environments. It is a challenge to develop a field device that not only is easy to install and maintain, have a long enough life length but also withstand this tough environment.

Problem description

Why is the information from installed Field Devices not already available? Modern process control systems often have the facility to pass HART commands through the I/O modules so that instrument configuration can be modified at the host system level. Remote access to HART instruments at the HOST system has been available for years however because of large number of brown field installations with a legacy communication architecture it is estimated that less than 10% of the entire population of Field Devices is connected so that all the information it provides is made available to the higher level system (See Figure 3.22) for a picture of a system). To get access to the information you need to wire in a HART multiplexor which is difficult to do and normally require a plant shutdown.

Integrated operations

With better connectivity to Field Devices better concepts for safe and cost-effective operations of facilities can be developed which is for both environmental and business reasons extremely important for the Oil & Gas industry.

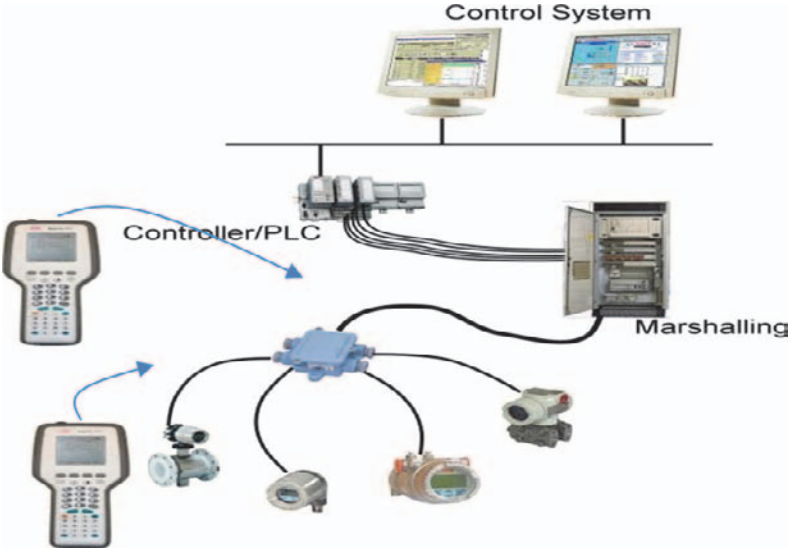

Fig. 3.22 4-20 mA HART has been available since 1990 and is mainly used for instrument commissioning where an engineer connects a hand held at the instrument to configure parameters.

Therefore Statoil, ABB, IBM, Aker Kvaerner and SKF joined forces in an R&D effort known as the CORD project in the beginning of the 2000's to develop new technology for more efficient operation of oil and gas field. The objective was to develop technology, processes and knowledge to extend the lifetime of Statoil's oil and gas fields, and thus improve the recovery factor. It was to evaluate, test and apply new and open standardized communication system architectures that allow handling increased amount of data from field devices to corporate systems in a cost-efficient and reliable manner.

The vision did not stop at the Field Devices but ambition is also to make the maintenance workplace accessible both at site as well as in the onshore operations center. Information should be possible to share both with internal as well as with external experts, i.e., experts from the product or system manufacturer thus facilitating co-operation between user groups and between different locations.

Potential with wireless

Much of the envisioned solutions only become possible with wireless communication. Wireless technologies have undergone various industrial trials over the last years, which have demonstrated that wireless communication can be

deployed in a wide variety of use cases, ranging from monitoring to safety critical applications. The main obstacle for a rapid adoption of wireless technologies is no longer the lack of suitable technologies; rather it's the lack of established industrial standards. Without standards, there is no effective means to achieve the interoperable, multi-vendor solutions which is required by customers. In addition, as many technologies operate in the same frequency band, standards are also required to ensure co-existence of wireless technologies (as wireless is an open medium).

The first wireless standards for process automation emerged only some years ago but already in 2002 the CORD project started investigating the possibility to do wireless condition monitoring on small AC motors. The project had mapped degradation mechanisms of these motors by interviewing specialists from the Oil companies and found that the most common and costly failure modes were bearing breakdown due to vibration and insulation failure. In 2004 the project tried to identify and assess different technologies and techniques to monitor the degradation mechanisms and the conclusion was that none of the existing "off-the-shelf" condition monitoring systems seemed to meet the requirements. In 2005 the project started to evaluate if and how the monitoring could be achieved by utilizing micro technology and in 2006 the spin-off project Wireless Condition Monitoring project was formed.

Why Motors

Why was condition monitoring of small AC motors selected? Some of the small AC motors on an oil rig are highly critical with respect to regularity, some are critical with respect to safety if for instance placed in EX (explosion proof) zone. Larger machines are normally always monitored but for these smaller AC motors the then prevailing maintenance strategy was "run-to-failure" due to their high numbers — of up to 1000 units per offshore installation — and the cost associated with monitoring them. A failure leads to high maintenance costs estimated to approximately 10 000 € per motor and per repair with a bearing failure being the most critical, causing the larger cost. The definition of AC motors is that they are below 400 kW in size and normally run at around 3000 r/min. At an oil rig these are the motors used to drive equipment such as pumps, air compressors and fans.

WiMon 100

The outcome of the project was an ABB product called the WiMon 100. It is a battery operated device with an expected lifetime of five years that intends to reduce the cost of maintenance as well as extend the lifetime of electric motors. The sensor is Ex-proof and is ideal for use in the offshore sector. In principle, however, it can be used in all industrial sectors with the same benefits. The product uses the new WirelessHART™ communications protocol, which was ratified in September 2007. The Wireless Vibration system delivers a cost effective, secure and reliable data acquisition, analysis, and sharing of real time information. The small, autonomous WiMon 100 unit comprises a vibration sensor, temperature sensor, long-life battery and a WirelessHART™ radio.

WiMon 100 was jointly developed by ABB researchers in Norway and Sweden, in cooperation with SKF Reliability Systems and SINTEF (an independent research organization based in Norway). The project received financial support from the Research Council of Norway through its Petromaks and DEMO2000 programmers, as well as from several oil companies including Statoil and BP.

Due to the cost efficiency, small size and ease of mounting and installation of the WiMon 100 sensor, continuous vibration monitoring can be realized for all types of rotating machines. WiMon 100 units form a mesh communication network; providing a secure, reliable and redundant path from WiMon 100 sensor to a gateway and onwards to monitoring and analysis tools (the central system). The central system (PC, network, DCS…) performs the necessary data analysis and storage and makes data available in real time.

The system (visualized in Figure 3.23) also contains a WirelessHART™ gateway that coordinates the sensor communication and manages the network security. The gateway device converts wireless device data to a format that is compatible with the wired automation systems.

A WiMon Data Manager provides the following main functionalities: a system browser, a system for commissioning and maintenance support (including firmware upgrade), automated data acquisition and storage of waveforms and dynamic data (velocity, envelope and temperature) in an OPC server, an operator interface for showing vibration waveforms and trends and temperatures and a waveform export tool for the interfacing of analysis packages like the ABB Analyst.

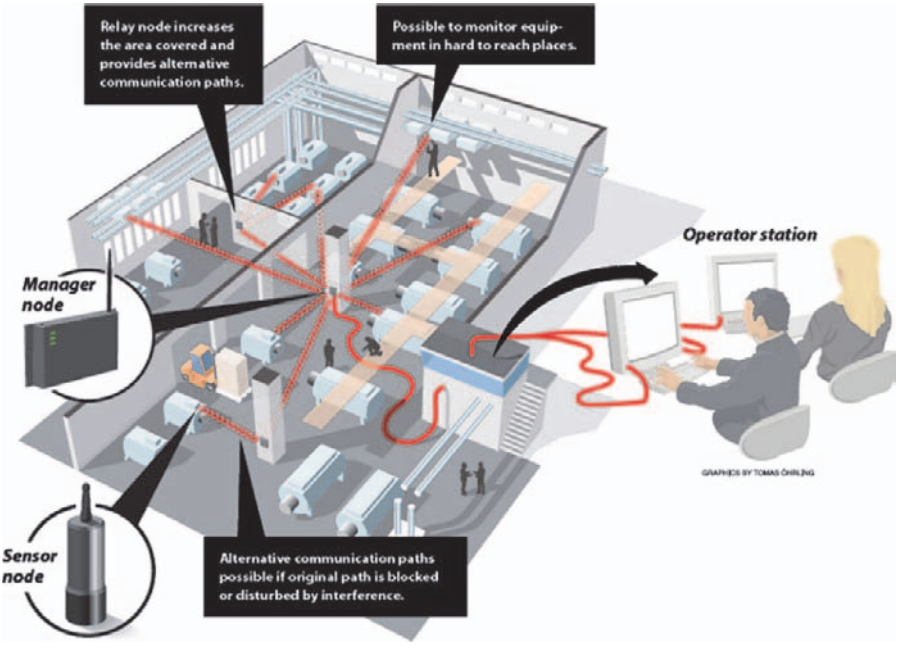
Relay node increases the area covered and provides alternative communication paths.
Possible to monitor equipment in hard to reach places.
Operator station
Manager node
Sensor node
Alternative communication paths possible if original path is blocked or disturbed by interference.
GRAPHICS BY TOMAS ÖHRLING

Fig. 3.23 A possible deployment of the WiMon 100 sensor and gateway.

The WiMon has been successfully deployed on oil rigs for the North Sea and more wireless Field Devices, also energy harvesting without the need of batteries, are developed and marketed by ABB. More and more information is made available to the benefit of a more efficient and environmental friendly operation of the future oil and gas fields!

3.10 Opinions on IoT Application and Value for Industry

At a recent international workshop on IoT application and value creation for industry [2] a quick survey was done asking participants at the workshop on their opinion on value creation using industry IoT applications.

The structure of the survey, as shown in Figure 3.24, has asked on IoT areas of application and expected time evolution, technologies and challenges. The respondents have been form academia, research, public/governmental and industry and although the number of respondents was limited it is worth looking at the expressed opinions such as those detailed in the following.

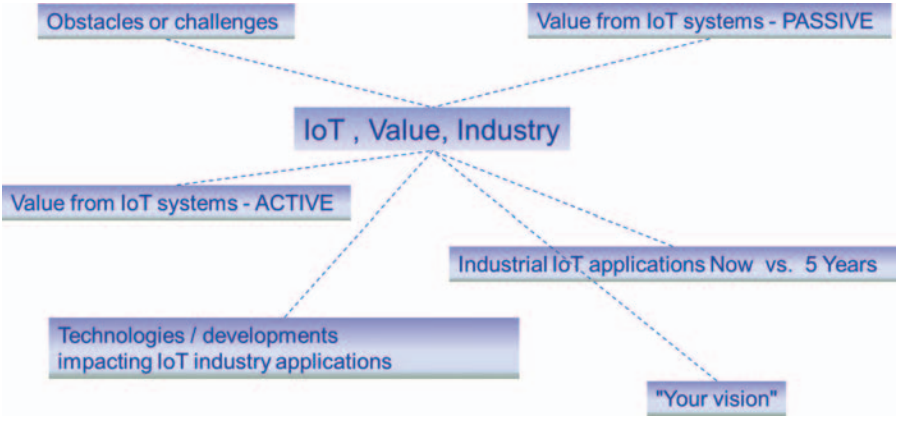
Obstacles or challenges
Value from IoT systems - PASSIVE
IoT , Value, Industry
Value from IoT systems - ACTIVE
Industrial IoT applications Now vs. 5 Years
Technologies / developments
impacting IoT industry applications
"Your vision"

Fig. 3.24 IoT small survey structure.

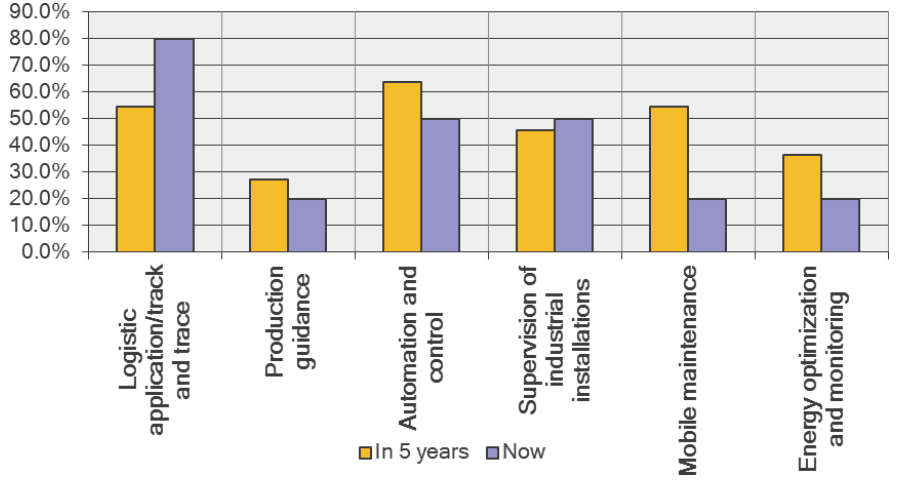

Fig. 3.25 Main areas of industrial IoT applications — presently and in 5 years.

The opinions expressed by respondents regarding the main areas of IoT industrial applications, as today versus expected in 5 years from now are shown in Figure 3.25. As expected the logistic applications are dominating now however a strong increase is expected in mobile maintenance, energy optimization and supervision of industrial installations.

Opinion on industry areas expected to benefit most from IoT applications are shown in the Figure 3.26. Logistics and supply chains applications

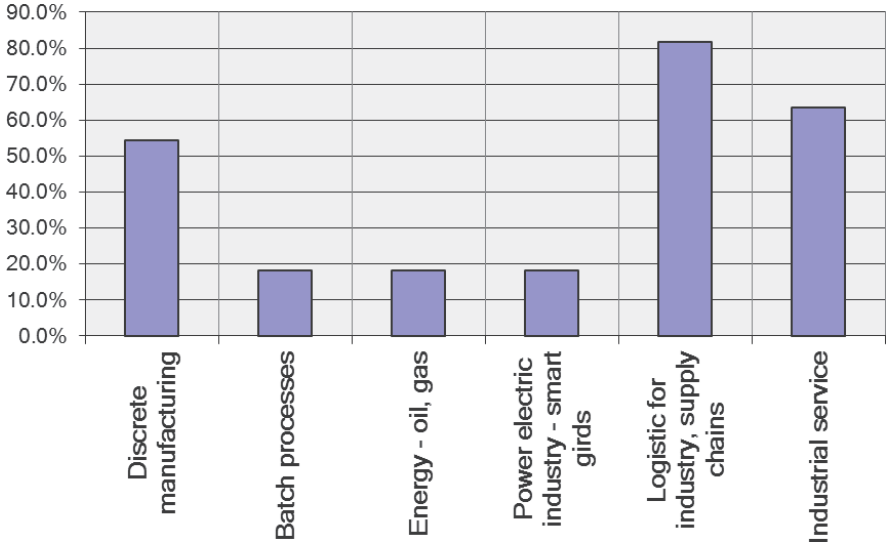

Fig. 3.26 Industry areas are expected to have most important benefit form IoT applications.

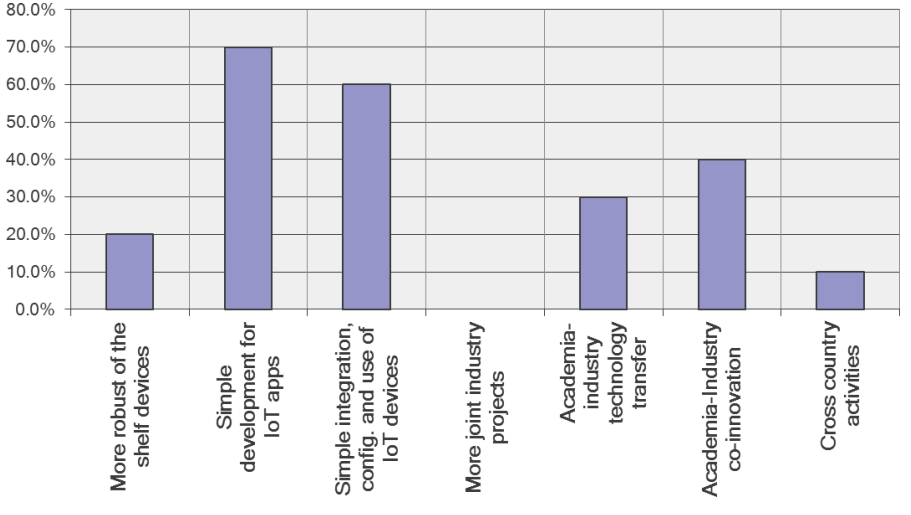

Fig. 3.27 How to create more value form IoT applications.

for industry are still the strongest followed by industrial service and discrete manufacturing.

Yet another key question was on how to create more value form IoT applications. The responses are in Figure 3.27. The top two responses are referring

to the need for simple development tools and methods for IoT applications, more in the sense of moving away for a lot of tailored solutions. Also the need for simple integration, deployment, configuration and use of IoT devices was seen as an important aspect to ease IoT application installation, configuration and practical industrial use. As a means to achieve this aspect of co-innovation academia- industry and quick technology transfer has been emphasized by respondents.

3.11 Conclusions

IoT applications exist and are rapidly developing in the industrial sector too, and are very diverse. IoT industrial applications can create value for industry. Examples are presented in the domains of optimizing business process flows based on the analysis if big data, optimizing processes based on smart tags and smart objects and the implementation of ad-hoc predictive maintenance applications as brown field IoT and in the hard environment of oil and gas industry based on sensor networks. The examples clearly show that the main mechanism to create value from IoT technology is to generate actual and fine grained information from real world and to optimize business and technological processes based on it. Handling and managing the data but especially extracting relevant information and correlating IoT data with other factory information and processes will determine the success of IoT industrial applications. The increasing number of technical contributions using IoT demonstrate that technologies are evolving and there is a learning and application process supported by standardization efforts. Robustness, standardization, easy installation, configuration and servicing are essential to keep IoT systems operational and hence offering value for the industry operation and services. From an industry point of view value creation from IoT applications and sustainability are essential and will influence the use of IoT technologies in the industry, on a larger scale, in the coming years.

References

[1] Industry 4.0, http://www.bitkom.org/74733.aspx.
[2] Industry workshop, The 3rd Int. Conference on the Internet of Things, Wuxi, http://www.iot-conference.org/iot2012/pagedf0b.html?id=162, China, 24–26. Oct. 2012,
[3] CISCO on Internet of Everything, Value at stake in the IoE economy, 13. Feb. 2013, http://www.slideshare.net/CiscoIBSG/internet-of-everything-ioe-economy#

[4] Building Value from Visibility, Forrester Consulting, June 2012, survey on behalf of Zebra.
[5] Ackoff, R. L. and F. E. Emery. On Purposeful Systems — An Interdisciplinary Analysis of Individual And Social Behavior As a System of Purposeful Events. 4th Edition, Transaction Publishers, New Jersey, 2009.
[6] Weiser, M. The Computer for the 21st Century. In: *Scientific American*, Vol. 265(3)/1991, S. 94–104.
[7] Villa, M. et al.: IoT@Work D1.1 — State of the art and functional requirements in manufacturing and automation. Report, https://www.iot-at-work.eu/data/D1.1_SotA_Requirements_final.pdf, 2010.
[8] Gorecky, D., S. F. Worgan, G. Meixner. COGNITO-A Cognitive Assistance and Training System for Manual Tasks in Industry. In: Proc. of 29th European Conf. on Cognitive Ergonomics. European Conference on Cognitive Ergonomics (ECCE-11), August 24–26, Rostock, Germany, 2011.
[9] P. Stephan, et al. "Product-Mediated Communication through Digital Object Memories in Heterogeneous Value Chains," In: *Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications*, Mannheim, Germany, 29.03.-02.04.2010.
[10] Zühlke, D. SmartFactory — Towards a factory-of-things. *IFAC Annual Reviews in Control*, Vol. 34(1)/2010.
[11] Fantana, Nicolaie L. and Till Riedel. 2010. A pragmatic architecture for ad-hoc sensing and servicing of industrial machinery. In Networked Sensing Systems (INSS), 2010 Seventh International Conference on, 165–168.
[12] Internet Connected Devices About to Pass the 5 Billion Milestone. In: Business Wire (2010).
[13] Riedel, T., N. Fantana, A. Genaid, D. Yordanov, H.R. Schmidtke, and M. Beigl. 2010. Using web service gateways and code generation for sustainable IoT system development. In Internet of Things (IOT), 2010, 1–8.
[14] Jammes, F. and Smit, H., "Service-oriented paradigms in industrial automation," *IEEE Trans. on Industrial Informatics*, vol. 1, 2005, pp. 62ff.
[15] Kuhn, A. and G. Bandow. (2007). Trends und Chances for the Maintenance Industry. Management Circle Summit Maintenance 2007. München, 2007.
[16] Wauer, M., J. Meinecke, D. Schuster, A. Konzag, M. Aleksy, and T. Riedel. "Semantic Federation of Product Information from Structured and Unstructured Sources" IJBDCN 7(2): 69–97 (2011).
[17] Matthias Berning, Till Riedel, NicolaieFantana and Michael Beigl: *Augmented Service in the Factory of the Future*, in Adjunct Proceedings of INSS2012, Antwerp, June 2012.
[18] [Womack, 1990] James P.; Daniel T. Jones, and Daniel Roos (1990). The Machine That Changed the World (Schribner, 1990).
[19] [Auto-ID Cloud of Things] http://web.mit.edu/newsoffice/2012/auto-id-cloud-of-things-big-data.html
[20] [ISO18000-6C] http://www.gs1.org/about/gs1_and_iso1
[21] [IGR] INTERPOL Global Register unveiled at Google Ideas INFO summit, Lyon, Interpol Red Notice. 2012.
[22] [NXP; Quanray] Tagging Small Objects using RFID antenna in silicon chips; Hao Min RFID Journal; http://www.rfidjournal.com/articles/view?3716.

[23] [Brynolfsson, 2012] Big Data: The Management Revolution; Center for Digital Business; (December 12, 2012) MIT Sloan School; http://digital.mit.edu/bigdata/index.html
[24] [BigData@CSAIL]; http://bigdata.csail.mit.edu/
[25] [Boer, 2013] Managing Risk in the Biopharma Supply Chain; Laurent Boer, VP of Global Distribution & Logistics, Genzyme; January 25, 2013; http://www.supplychainbrain.com/content/index.php?id=5032&cHash=081010&tx_ttnews[tt_news]=18986
[26] [2012 Auto-ID Big Data] 2012 MIT Auto-ID Labs Big Data Conference; http://ilp.mit.edu/conference.jsp?confid=70&tabname=overview
[27] [BIOMAN] http://cbi.mit.edu/research-overview/bioman/
[28] [Miles, 2012] "Application Programming Interfaces (API's) for the Biologics Supply Chain," Stephen Miles, PDA/FDA Pharmaceutical Supply Chain Conference; November 13-14, 2012; Bethesda, Maryland; http://www.pda.org/Presentation/PDAFDA-Pharmaceutical-Supply-Chain-Conference.aspx
[29] [WHO, 2010] Bulletin of the World Health Organization. Growing Threat from Counterfeit Medicines. April 2010. Vol. 88(4), pp. 241–320.
[30] [IDC Tech Insight, 2010] https://idc-insights-community.com/health/life-sciences/revenue-leakage-pharmas-11-billion-problem.
[31] 4th Annual Biomanufacturing Summit: Implementing Innovation in Biomanufacturing: The Hurdles and the Opportunities; MIT Center for Biomedical Innovation; (November 18, 2011, MIT, Cambridge MA).
[32] "Managing Risk in the Biopharma Supply Chain;" Supply Chain Brain; Laurent Boer, VP of Global Distribution & Logistics, Genzyme; January 25, 2013

4

Internet of Things Privacy, Security and Governance

Gianmarco Baldini[1], Trevor Peirce[2], Marcus Handte[3], Domenico Rotondi[4], Sergio Gusmeroli[5], Salvatore Piccione[6], Bertrand Copigneaux[7], Franck Le Gall[8], Foued Melakessou[9], Philippe Smadja[10], Alexandru Serbanati[11], and Julinda Stefa[12]

[1]*Joint Research Centre — European Commission, Italy*
[2]*AVANTA Global SPRL, Belgium*
[3]*Universität Duisburg-Essen, Germany*
[4]*TXT e-solutions S.p.A., Italy*
[5]*TXT e-solutions S.p.A., Italy*
[6]*TXT e-solutions S.p.A., Italy*
[7]*Inno TSD, France*
[8]*Inno TSD, France*
[9]*University of Luxemburg, Luxemburg*
[10]*Gemalto, France*
[11]*Sapienza University of Rome, Italy*
[12]*Sapienza University of Rome, Italy*

4.1 Introduction

Internet of Things (IoT) is broad term, which indicates the concept that increasingly pervasive connected devices (embedded within, attached to or related to "Things") will support various applications to enhance the awareness and the capabilities of users. For example, users will be able to interact with home automation systems to remotely control the heating or the alarm system.

Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, 207–224.
© 2013 *River Publishers. All rights reserved.*

The possibility of implementing "intelligence" in these pervasive systems and applications has also suggested the definition of "Smart" contexts, where digital and real-word objects cooperate in a cognitive and autonomic way to fulfil specific goals in a more efficient way than basic systems implemented on static rules and logic. While full cognitive and autonomic systems may still be years away, there are many automated processes and automated Internet process which we take for granted every day. So why should the Internet of Things (IoT) require special attention when it comes to privacy, security and governance? Doesn't the established Internet have these matters dealt with sufficiently already, given that through just about every smartphone anywhere there are already a wide variety of sensors capturing information which we share on the Internet e.g. photos, videos, etc.? Why is IoT any different?

Firstly IoT is different because it will be possible and likely that objects will autonomously manage their connections with the Internet or, this will be done upon the request of someone or something remotely. When someone shares a video or a photo taken on their mobile phone over the Internet they "call the shots". With IoT potentially someone else is in charge. For reasons largely similar to this, the topics of privacy, security and governance are very important if not vital to the success of IoT in order to establish and maintain stakeholder trust and confidence. Yes, there is a large overlap between IoT and Internet in many areas pertaining to trust however IoT brings many new specific dimensions too.

The adoption of IoT essentially depends upon trust. Moreover this trust must be established and maintained with respect to a broad group of stakeholders otherwise IoT will face, to some degree or other, challenges which may restrict adoption scope or delay its timing. Note that with social media you make the conscious choice to publish; some IoT applications may adopt the same or similar model but there may be other instances or applications where this will not be the case. This remote control is not essentially bad. For example if you were incapacitated due to an accident it could be advantageous that rescue services would be able to access objects in your environment to locate you or communicate with you. However if these devices were configured to automatically inform your children what presents had been bought or not bought this could spoil much of the excitement of receiving gifts. Facebook's withdrawn Beacon[1] service was accused of this when shoppers'

[1] http://en.wikipedia.org/wiki/Facebook_Beacon

purchases were automatically published on-line resulting in a public outcry and class-action in the US post-holidays (Christmas). There are also potential ethical issues if essential services oblige you to use IoT connected health monitoring devices. Also a number of Internet services are already struggling with the ethical issues of capturing and publishing information affecting 3rd parties where appropriate permissions have not been sought from the 3rd parties involved e.g. Street View.[2] Trust, privacy and governance aspects of IoT rely for the most part upon security [1]. Security in its broadest definitions includes health and wellbeing as well as other forms of protection. These aspects need to be viewed from the perspectives of the majority if not all the principle stakeholder groups and extended to include the relevant influencing and influenced elements of the general environment. Today from the European Commission's perspective the essential focus for security is the protection of health and, the avoidance of potential super-power control being established by enterprises. The objectives are not currently focused upon seeking specific IoT measures to deter cyber-crime, cyber-warfare nor terrorism. Without sufficient IoT security it is highly likely that some applications will more resemble the Intranet of Things rather than the Internet of Things (see [2]) as users seek to place their own proprietary protection barriers and thus frustrating broad interoperability. Many of the device connections to the Internet today more closely resemble the Intranet of Things which differs dramatically from the vision for the Internet of Things, the latter being a much more open and interoperable environment allowing in theory the connection with many more objects and with their multiple IoT compatible devices.

The future of IoT is not only influenced by users. The potential autonomy of IoT or lack of control over IoT by those it impacts will doubtless generate IoT adoption resistance potentially manifested by public protests, negative publicity campaigns and actions by governments. Indeed many IoT foundation technologies have been influenced during the last 10 years by the developing concerns which have been labelled as "threats to privacy". Privacy itself is multi-dimensional. Popular definitions focus upon individual freedoms, or the "right to be left alone". In reality privacy encompasses the interests of individuals, informal groups and including all forms of organizations and is therefore a complex multidimensional subject.

[2] http://en.wikipedia.org/wiki/Google_Street_View

In an age of social media it is interesting to see growing examples of how industry groups and governments begin to encourage greater individual responsibility for protecting our own privacy, defending our virtual representation in order to protect our identity and diminish the challenges of real-world or virtual-world authentications and authorization processes. Through IoT this may become an increasingly 'hard sell' as individuals begin to realize that any efforts individuals take to protect their own identities have almost no influence due to the amounts of information smart objects are collecting and publishing on the Internet. Ideally IoT would provision for flexibility enabling it to be suitably synchronized with the evolution of the development and use of the wider Internet and the general real-world environment.

One specific challenge in IoT is the control of the information collected and distributed by mobile devices which are increasingly small and pervasive like RFID or future micro-nano sensors, which can be worn or distributed in the environment. In most cases, such devices have the capability of being wireless connected and accessible. In this context, the challenge is to ensure that the information collected and stored by micro/nano-RFID and micro/nano sensors should be visible only to authorized users (e.g., the owner or user of the object) otherwise there could be a breach of security or privacy. For example, the owner of a luxury good may not want anybody to know that the luxury good is in a suitcase. The watch in the suitcase may be hidden from view, but it can be easily tracked and identified through wireless communication. In a similar way, the information collected by the body sensors applied to an elderly person should not be accessible by other persons apart from the doctor. Access control mechanisms for these wireless devices should be implemented and deployed in the market, but security and privacy solutions are not easy to implement in micro-nano devices because of the limitations in computing power and storage. At the same time, security and privacy should not hamper business development of micro-nano technologies. Keys management and deployment can also be complex to implement. Trade-offs should be identified and described. These are goals for research activity.

One aspect which often gets overlooked particularly frequently by those of us who entered adulthood before the year 1990 is the importance of the virtual-world. Today the virtual identities of children are as important to them if not more so than their real-world identities. Within the virtual-world there exists most if not all of the things we find in the real-world including objects,

machines, money, etc. IoT includes the real and virtual-worlds and indeed it is capable of establishing an important bridge between the two. This bridge is likely to grow and become more relevant in the life of citizen in the future. New devices like Google Glass or future Intelligent Transportation Systems (ITS) applications in cars will propose "augmented reality" where the integration of digital and real-word information is used to compose sophisticated applications. This trend highlights even more the need for security and privacy, because data breaches in the virtual-world can have consequences in the real-world. In some contexts and applications, security and privacy threats can even become safety threats with more dramatic consequences for the lives of the citizen. As a conceptual example, actuators in the real-world may be set remotely within a "smart house" to provoke fires or flooding.

4.2 Overview of Activity Chain 05 — Governance, Privacy and Security Issues

The European Research Cluster on the Internet of Things has created a number of activity chains to favour close cooperation between the projects addressing IoT topics and to form an arena for exchange of ideas and open dialog on important research challenges. The activity chains are defined as work streams that group together partners or specific participants from partners around well-defined technical activities that will result into at least one output or delivery that will be used in addressing the IERC objectives. IERC Activity Chain 05 is a cross-project activity focused on making a valued contribution to IoT privacy, security and governance among the EC funded research projects in the area of Internet of Things. As described in [3], the three aspects are closely interlinked "Privacy, security and competition have been identified as the main issues related to IOT Governance, however those issues should not be discussed in a separate or isolated way" (from [3]). In the same reference, it was also highlighted the challenge to define a common agreed definition for Governance of IoT. In a similar way, the concepts of security and privacy do not have a uniform definition in literature even if there is a common agreement on these concepts. Overall, the main objective of the Activity Chain 05 is to identify research challenges and topics, which could make IoT more secure for users (i.e. citizen, business and government), to guarantee the privacy of users and support the confident, successful and trusted development of

the IoT market. In comparison to IoT initiatives in Europe or at a global level (e.g., IGF), Activity Chain 05 does not define government policies but focuses upon research (which could eventually be used to support policies or standardization activities). The following sections provide an overview of some contributions which European Commission funded projects associated with Activity Chain 05 have made to IoT privacy, security and governance.

4.3 Contribution From FP7 Projects

4.3.1 FP7 iCore Access Framework (iCore Contribution)

The iCore cognitive framework is based on the principle that any real world object and any digital object that is available, accessible, observable or controllable can have a virtual representation in the "Internet of Things", which is called Virtual Object (VO). The virtual objects (VOs) are primarily targeted to the abstraction of technological heterogeneity and include semantic description of functionality that enables situation-aware selection and use of objects. Composite virtual objects (CVOs) use the services of virtual objects. A CVO is a cognitive mash-up of semantically interoperable VOs that renders services in accordance with the user/stakeholder perspectives and the application requirements.

The overall layered approach of the iCore project is provided in Figure 4.1.

The first cognitive management layer (VO level cognitive framework) is responsible for managing the VOs throughout their lifecycle, ensuring reliability of the link to the real world object/entity (e.g., sensors, actuators, devices, etc.). They represent for example, in a logistic related scenario, tracking temperature controlled goods transport, individual goods boxes are represented by VOs the container transported by a truck is a VO as is the truck itself. IoT related applications can interface for different service reasons each of these VOs separately.

The second cognitive management layer (CVO level cognitive framework) is responsible for composing the VOs in Composite VO. CVOs will be using the services of VO to compose more sophisticated objects. In our example, the combination of the truck and the transported goods is represented in the cognitive framework as a CVO.

The third level (User level cognitive framework) is responsible for interaction with User/stakeholders. The cognitive management frameworks will

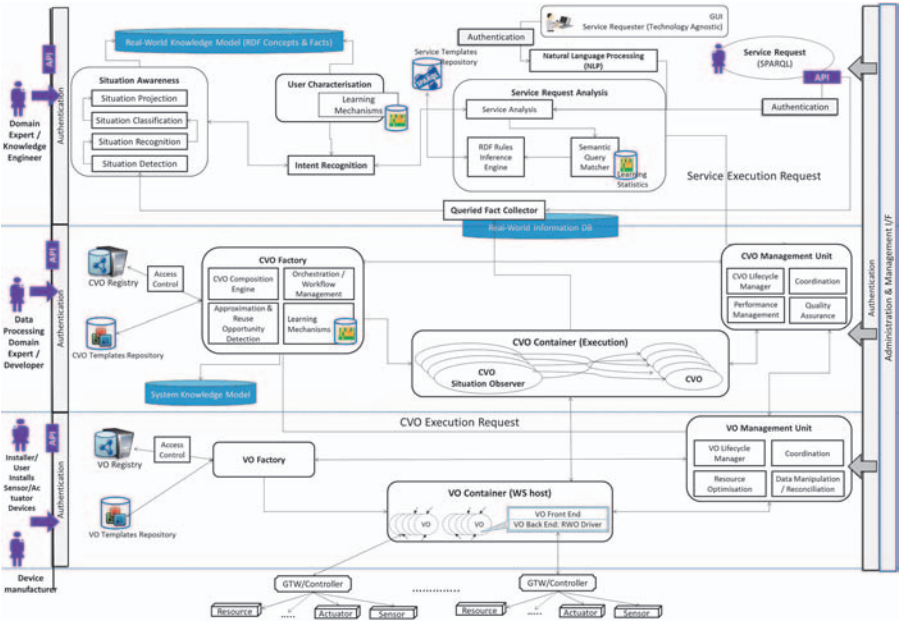

Fig. 4.1 iCore framework.

record the users needs and requirements (e.g., human intentions) by collecting and analyzing the user profiles, stakeholders contracts (e.g., Service Level Agreements) and will create/activate relevant VO/CVOs on behalf of the users.

4.3.2 IoT@Work Capability Based Access Control System (IoT@Work Contribution)

The Internet of Things (IoT) envisages new security challenges, including in the area of access control that can hardly be met by existing security solutions. Indeed, IoT is a more demanding environment in terms of scalability and manageability due both to the potentially unbounded number of things (resources and subjects), the expected most relevant need to support the orchestration and integration of different services, the relevance of short-lived, often casual and/or spontaneous interaction patterns, the relevance of contexts, etc.

In the following we shortly provide a description of the Capability Based Access Control (in the following referred to as CapBAC) system developed

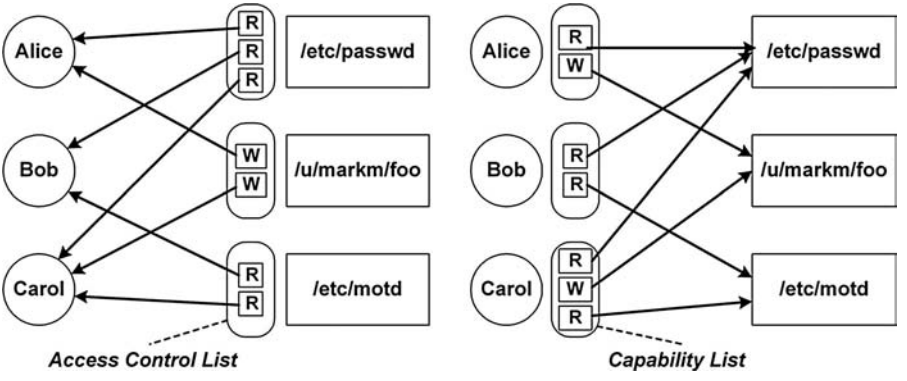

Fig. 4.2 ACL vs Capability-based authorization models.

within the EU FP7 IoT@Work project. The CapBAC is devised according to the capability based authorization model in which a capability is a communicable, unforgeable token of authority. This token uniquely identifies the granted right(s), the object on which the right(s) can be exercised and the subject that can exercise it/them. As depicted in Figure 4.2, a capability based system reverses the traditional approach being now the user in charge of presenting his/her/its authorization token to the service provider, while in a traditional ACL or RBAC system it is the service provider that has to check if the user is, directly or indirectly, authorized to perform the requested operation on the requested resource.

The CapBAC system borrows ideas and approaches from previous works (see [4]) extending and adapting them to IoT requirements and, specifically, the ones envisaged by the IoT@Work project. The CapBAC provides the following additional features that constitute the essential innovation over previous capability based techniques: a) Delegation support: a subject can grant access rights to another subject, as well as grant the right to further delegate all or part of the granted rights. The delegation depth can be controlled at each stage; b) Capability revocation: capabilities can be revoked by properly authorized subjects, therefore solving one of the issues of capability based approaches in distributed environments; c) Information granularity: the service provider can refine its behavior and the data it has to provide according to what is stated in the capability token. Figure 4.3 exemplifies the usage of a capability based access control approach to manage a simple situation: Bob has to go

on holidays and his house needs some housekeeping while he is away. Dave offered to take care of Bob's house for his holiday's period. Bob provides to Dave an access token that: a) Identifies Dave has the only subject entitled to use the token, b) States what Dave can actually perform c) States for how many days Dave can do these actions.

Bob and Dave do not need to establish trust relationships among their authentication and authorizations systems. Bob's house appliance recognizes the access token created by Bob and Dave has only to prove that he is the subject (grantee) identified by the capability token as entitled to do specific housekeeping activities for the holidays period. The above mechanism is very intuitive, easy to understand and easy to use. CapBAC is well suited to manufacturing contexts where there are many subjects, internal (e.g. workers, production supervisors) and external (e.g. suppliers, maintainers), that need access both directly (e.g. via mobile or desktop computing sets) or indirectly (e.g. via application services) to devices, data and services in the manufacturing plant. Most of, if not all, these elements require enforcement of strictly access control policies and finer-graded access control, and, at the same time, a management effort that has to be decoupled from the number of managed resources or subjects, especially when many subjects are external ones.

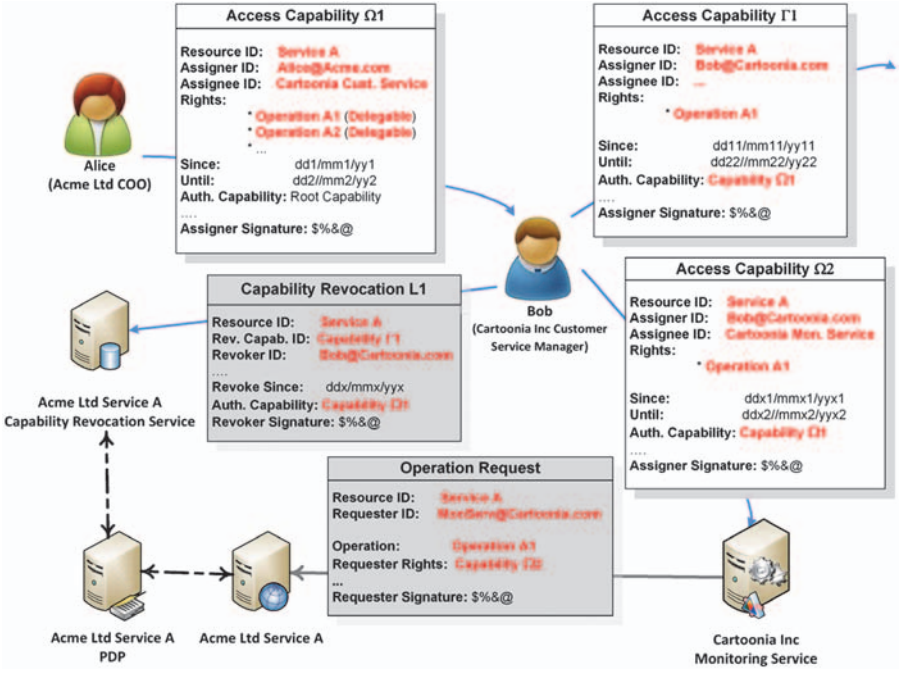

Fig. 4.4 Capability-based authorization architectural components and their interactions.

The CapBAC architectural elements can be shortly characterized as follows (see Figure 4.4):

- The resource object of the capability (Service A in Figure 4.4); it can be a specific data or device, a service or any accessible element that can be univocally identified and/or actable on (like resource);
- The authorization capability that details the granted rights (and which ones can be delegated and, in case, their delegation depths), the resource on which those rights can be exercised, the grantee's identity, as well as additional information (e.g. capability validity period, XACML conditions, etc.). An authorization capability is valid as specified within the capability itself or until it is explicitly revoked;
- The capability revocation is used to revoke one or more capabilities. Like a capability, a capability revocation is a communicable object a subject, having specific rights (e.g. the revoker must be an

ancestor in the delegation path of the revoked capability), creates to inform the service in charge of managing the resource that specific capabilities have to be considered no more valid;

- The service/operation request is the service request as envisaged by the provided service with the only additional characteristics to refer or include, in an unforgeable way, a capability. For example, for a RESTful service, an HTTP GET request on one of the exposed REST resource has to simply include the capability and its proof of ownership to use our access control mechanism;
- The PDP (Policy Decision Point) is a resource-agnostic service in charge of managing resource access request validation and decision. In the CapBAC environment it deals with the validation of the access rights granted in the capability against local policies and checking the revocation status of the capabilities in the delegation chain;
- The resource manager is the service that manages service/access requests for/to the identified resource. The resource manager checks the acceptability of the capability token shipped with the service request as well as the validity and congruence of the requested service/operation against the presented capability. It acts as an XACML Policy Enforcement Point (PEP) which consider the validation result of the PDP;
- The revocation service is in charge of managing capability revocations.

4.3.3 GAMBAS Adaptive Middleware (GAMBAS Contribution)

The GAMBAS project develops an innovative and adaptive middleware to enable the privacy-preserving and automated utilization of behaviour-driven services that adapt autonomously to the context of users. In contrast to today's mobile information access, which is primarily realized by on-demand searches via mobile browsers or via mobile apps, the middleware envisioned by GAMBAS will enable proactive access to the right information at the right point in time. As a result, the context-aware automation enabled by the GAMBAS middleware will create a seamless and less distractive experience for its users while reducing the complexity of application development.

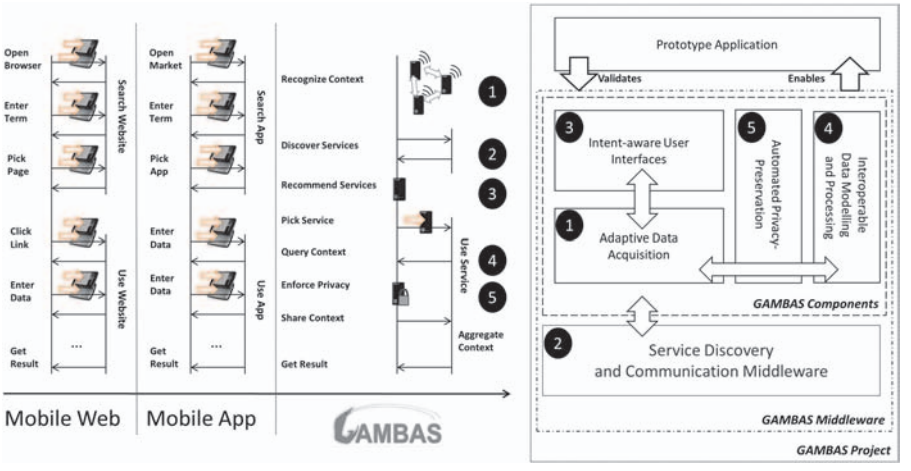

Fig. 4.5 GAMBAS middleware.

As indicated in Figure 4.5, the core innovations realized by GAMBAS are the development of models and infrastructures to support the interoperable representation and scalable processing of context, the development of a generic, yet resource-efficient framework to enable the multimodal recognition of the user's context, protocols and mechanisms to enforce the user's privacy as well as user interface concepts to optimize the interaction with behaviour-driven services.

From a security and privacy perspective, the developments in GAMBAS are centred on a secure distributed architecture in which data acquisition, data storage and data processing are tightly controlled by the user. Thereby, security and privacy is based on the following elements.

- Personal acquisition and local storage: The primary means of data acquisition in GAMBAS are personal Internet-connected objects that are owned by a particular user such as a user's mobile phone, tablet, laptop, etc. The data acquired through the built-in sensors of these devices is stored locally such that the user remains in full control. Thereby, it is noteworthy that the middleware provides mechanisms to disable particular subsets of sensors in order to prevent the accumulation of data that a user may not want to collect and store at all.

- Anonymised data discovery: In order to enable the sharing of data among the devices of a single user or a group of users, the data storages on the local device can be connected to form a distributed data processing system. To enable this, the GAMBAS middleware introduces a data discovery system that makes use of pseudonyms to avoid revealing the user's identity. The pseudonyms can be synchronized in automated fashion with a user defined group of legitimate persons such that it is possible to dynamically change them.
- Policy-based access control: To limit the access to the user's data, the networked data storages perform access control based on a policy that can be defined by a user. In order to reduce the configuration effort, the GAMBAS middleware encompasses a policy generator tool that can be used to derive the initial settings based on the user's sharing behaviour that he exhibits when using social services.
- Secure distributed query processing: On top of the resulting set of connected and access-controlled local data storages, the GAMBAS middleware enables distributed query processing in a secure manner. Towards this end, the query processing engine makes use of authentication mechanisms and encryption protocols that are bootstrapped by means of novel key exchange mechanisms that leverage the existing web-infrastructure that is already used by the users.

4.3.4 IoT-A Architecture (IoT-A Contribution)

Security is an important cornerstone for the Internet of Things (IoT). This is why, in the IoT-A project, we deemed as very important to thoroughly address security and privacy issues in various aspects. A set of requirements based on the input of external and internal stakeholders was used as a basis for the identification of the mechanisms and functionalities that guarantee user data privacy and integrity, user authentication, and trustworthiness of the system.

These functionalities were analysed and orchestrated in Functional Groups (FG) and Functional Components (FC) in the frame of WP1. High-level PS&T specifications were integrated in the frame of the IoT-A Architectural Reference Model (ARM) and then passed to vertical WPs dealing with communication protocols (WP3), infrastructure services (WP4) as well as hardware

aspects (WP5). Due to the highly heterogeneous environment provided by the IoT and the huge number of connected, (autonomous) devices foreseen by analysts, a strong focus was placed on scalability and interoperability.

The ARM document [5] paves the way for understanding and adopting the open architecture of IoT-A, as well as provides the overall definition of IoT security, privacy and trust design strategies that we adopted. Then, in WP3 we analysed the security of communication in the peripheral part of the IoT and its impact on the overall communication architecture. In this context we investigated HIP and HIP-BEX protocols, as well as considered issues like mobility, collaborative key establishment, and securing network entry with PANA/EAP.

Then, within the framework of WP4 [6] we developed a secure resolution infrastructure for IoT-A. It ensures privacy and security for the resolution functions as well as offers the basis for other security functionalities outside the resolution infrastructure. It controls the access to IoT resources, real world entities, and to the related information including their respective identifiers. In addition, the resolution infrastructure provides also support for pseudonymity: A user does not need to reveal his/her identity when using an IoT resource or a higher-level service. To achieve all this, various security components were developed (see Figure 4.6). They deal with authorization and authentication, key exchange and management, trust and reputation, and identity management.

Finally, WP5 deals with privacy and security at device level. In particular, it describes the mechanisms needed to authenticate RFID devices and to provide confidentiality of the communication between reader and tag. The PS&T features of the IoT-A architecture will be tested in the forthcoming IoT-A eHealth Use Case.

4.3.5 Governance, Security and Privacy in the Butler Project (Butler Contribution)

The goal of the BUTLER project is the creation of an experimental technical platform to support the development of the Internet of Things. The main specificity of the BUTLER approach is its targeted "horizontality": The vision behind BUTLER is that of a ubiquitous Internet of Things, affecting several

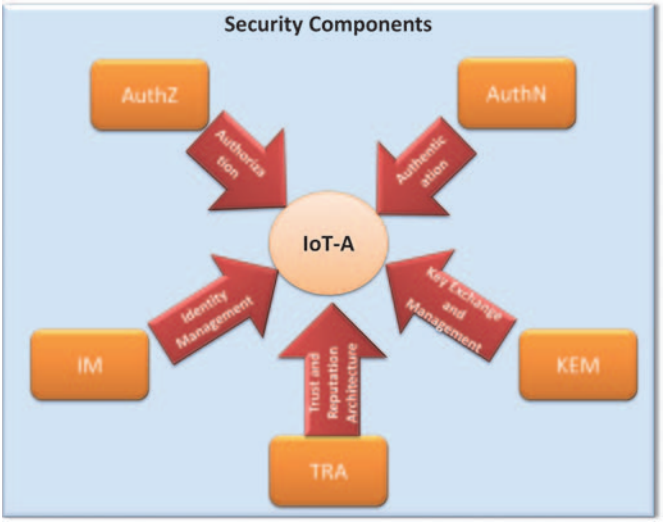

Fig. 4.6 Components for privacy and security in the IoT-A resolution infrastructure.

domains of our lives (health, energy, transports, cities, homes, shopping and business) all at once. The BUTLER platform must therefore be able to support different "Smart" domains, by providing them with communication, location and context awareness abilities, while guaranteeing their security and the privacy of the end users. The issue of security and privacy is therefore central in the BUTLER project and develops in several requirements, the main requirements relate to:

- Standard issues of data security, both at data storage level as at data communication level exists in IoT application. The diversity and multiplicity of the "things" connected by the internet of things, and of the data exchanged further amplifies and complicate these requirements.
- The application enabled by the Internet of Things may pose additional privacy issues in the use that is made of the data. From the collection of data by the applications (which should be conditioned by an "informed consent" agreement from the user), to the profiling, exchange and sharing of these data necessary to enable true "context awareness".

Data technical protection[3] mechanisms include two major aspects. One is the protection of the data at data storage, the other one the protection of the data at communication level. The protection of data at communication level is one the major area of research. Many communication protocols implement high level of end-to-end security including authentication, integrity and confidentiality. At communication level, the major issue is the deployment process of the security keys and the cost of the required hardware and software environment to run the security algorithms in efficient and secure way.

However, Privacy and Security do not only refer to security of the exchange of data over the network, but shall also include: (a) Protection of the accuracy of the data exchanged, (b) Protection of the server information, (c) Protection of the usage of the data by explicit, dynamic authorization mechanisms, (d) Selected disclosure of Data and (e) The implementation of "Transparency of data usage" policies.

The BUTLER project also addresses the Security and Privacy challenges from the point of view of their implication on business models. To specify the horizontal IoT platform envisioned in BUTLER, the project started from the gathering and analysis of the requirements from up to 70 use cases. The analysis of these use case not only produced requirements for the specification of the platform but also valuable information on the potential socio-economic impact of the deployment of an horizontal IoT and on the impact on the associated business models.

If treated accordingly, the ethics and privacy issues transforms from a threat to an opportunity. Better understanding of the service by the user increase acceptance and create trust in the service. This trust becomes a competitive advantage for the service provider that can become a corner stone of his business model. In turn the economic interest of the service providers for ethics and privacy issues, derived from this competitive advantage, becomes a guarantee for the user that his privacy will be respected. The BUTLER project research on the implication of the Ethics, Privacy and Data security on the business models and socio economic impact will be published in Deliverable 1.4 (May 2013) and Deliverable 1.3 (September 2014).

[3]An exhaustive study of the security enabling technologies is available in "D2.1 Requirements, Specification and Security Technologies for IoT Context-aware network". http://www.iot-butler.eu/download/deliverables

The involvement of end users in proof of concepts and field trials is another specificity of the BUTLER project. The end user involvement is key to validate not only the technical qualities of the BUTLER platform (technology feasibility, integration and scaling) but also to assess the perception of end user and their acceptance of the scenario envisioned for the future "horizontal" IoT.

However the involvement of end user in the scope of the project requires handling their data and privacy concerns carefully. The detailed specification of the field trials and proof of concept is described in Deliverable 1.2, (scheduled for end of May 2013). The following issues must be considered in the organization of end user involvement: (a) Technical security mechanisms must be set up to ensure the security and privacy of the participants. This involves secured data communication and storage, and in the scope of the BUTLER project is addressed by the enabling security technologies developed and integrated in the BUTLER platform; (b) The participants must be well informed of the scope and goal of the experiment. In the case of BUTLER, this involves specific efforts to explain the scope and goal of the project to a larger public; (c) The consent of the participants must be gathered based on the information communicated to them. The consent acknowledgment form must remind the participants of their possibility to refuse or withdraw without any negative impact for them; (d) finally both a feedback collection and a specific complaint process have been designed to offer the possibility to the participants to raise any issue identified.

4.4 Conclusions

IoT applications and supporting stakeholders can all mutually benefit from the establishing of a trusted IoT. Trust means establishing suitable provisions for privacy, security and governance. To put in place and maintain trust means fulfilling today's needs while providing sufficient future provisions to meet naturally evolving stakeholder requirements and expectations. Consensus necessary for the formation of successful standards and guidelines can only come through dialogue. Activity Chain 05 provides such a platform for information exchange and mutual understanding as well as in providing valued leadership. The research projects within Activity Chain 05 all contribute to advancing IoT adoption, some having universal IoT application value while others provide significant enhancements to specific IoT application groups. Making this

landscape clearer, identifying the gaps for further research as IoT develops and, assisting the progression of research towards standardization and adoption remain the principle challenges for Activity Chain 05. Another role for Activity Chain 05 is raising awareness and promoting adequate consideration of IoT privacy, security and governance within the other Activity Chains of the IERC and the wider stakeholder community.

References

[1] Roman, R., Najera, P., Lopez, J., "Securing the Internet of Things," *Computer* , vol. 44, no. 9, pp. 51, 58, Sept. 2011.

[2] Zorzi, M., Gluhak, A., Lange, S., Bassi, A., "From today's INTRAnet of things to a future INTERnet of things: a wireless- and mobility-related view," *IEEE Wireless Communications*, vol. 17, no. 6, pp. 44, 51, December 2010.

[3] Final Report of the EU IOT Task Force on IOT Governance. Brussels, November 14, 2012.

[4] Gusmeroli, S., Piccione, S., Rotondi, D., "IoT Access Control Issues: A Capability Based Approach," in *Proceedings of 6th Int. Conf. on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2012)*, pp. 787–792, July 2012.

[5] Carrez, F. (ed), Converged architectural reference model for the IoT, available at http://www.iot-a.eu/public/public-documents. Last accessed 10 May 2013.

[6] Gruschka, N., Gessner, D. (eds.), Concepts and Solutions for Privacy and Security in the Resolution Infrastructure, available at http://www.iot-a.eu/public/public-documents. Last accessed 10 May 2013.

5

Security and Privacy Challenge in Data Aggregation for the IoT in Smart Cities

Jens-Matthias Bohli[1], Peter Langendörfer[2], and Antonio F. Skarmeta[3]

[1]*NEC Lab Europe*
[2]*IHP MicroElectronics*
[3]*Universidad de Murcia, Spain*

Abstract

The Internet of the Future will be an essential part of the knowledge society and will provide new information-based business. The usage of the Internet of Things for large-scale, partially mission-critical systems creates the need to address trust and security functions adequately.

The vision of SMARTIE[1] (Secure and sMArter ciTIEs data management) is to create a distributed framework for IoT based applications sharing large volumes of heterogeneous information. This framework is envisioned to enable end-to-end security and trust in information delivery for decision-making purposes following data owner's privacy requirements. New challenges identified for privacy, trust and reliability are:

- Providing trust and quality-of-information in shared information models to enable re-use across many applications.
- Providing secure exchange of data between IoT devices and consumers of their information.
- Providing protection mechanisms for vulnerable devices.

[1]This work is partially funded by EU FP7 Project SMARTIE contract 609062.

Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, 225–244.
© 2013 *River Publishers. All rights reserved.*

SMARTIE will address these challenges within the context of Smart Cities. In this chapter we will present the SMARTIE focus on the security, trust and privacy of the Internet-of-Things infrastructure and the generated data. The dissemination of collected data and use of information must be protected to prevent harm to the control and management of the smart city infrastructure and to the citizen. Privacy-protection and access control to the data is necessary to convince data owners to share information in order to allow better services in the city. SMARTIE envisions a data-centric paradigm, which will offer highly scalable and secure information for smart city applications. The heart of this paradigm will be the "information management and services" plane as a unifying umbrella, which will operate above heterogeneous network devices and data sources and will provide advanced secure information services enabling powerful higher-layer applications.

5.1 Security, Privacy and Trust in Iot-Data-Platforms for Smart Cities

5.1.1 Overview

One of the main aims of Smart City technologies is to provide different optimization mechanisms for different aspects of data management. Data is gathered from various sources owned by different administrative domains. Noteworthy parts are data from public and private transportation providers, data from mobile users, captured for instance with their smart phones, surveillance data and videos from private and public organisations and a vast amount of sensors and meters, attached to machines and infrastructures, distributed throughout the city. All this information is stored in a variety of different places, for instance it can remain locally in the sensors or company internal databases, in social networks, in data storage located in private data centres or even in a public cloud storage service.

Figure 5.1 shows the components of a typical smart city information system. From this picture it is clearly visible that information needs to cross multiple administrative boundaries and can be used for multiple purposes — in fact it could be used for, at the time of gathering, unknown purposes. Also actuation decisions can be taken in a coordinated way between multiple control centres or data providers. Hence it is clear that there is a need of an information sharing platform in which data flows from various sources and from different

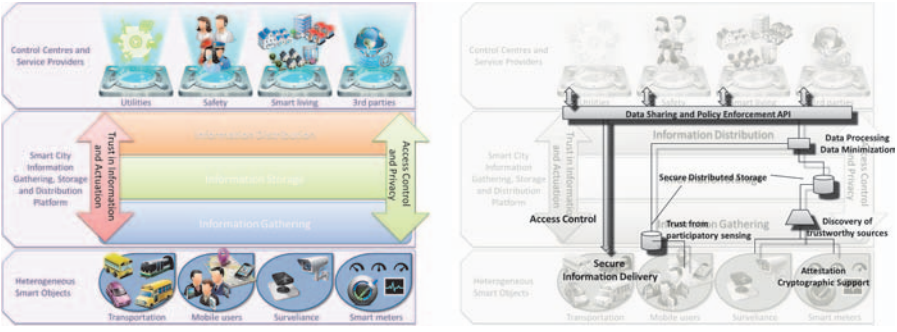

Fig. 5.1 Architectural components.

administrative boundaries need to be treated in a secure and privacy preserving way. To ensure this, security and privacy need to be part of the platform by design and may not be added later on. The design goal and challenge is allowing user/service control of the data accessible and at the same time providing solution for easily configured management of the process.

All parties involved in the overall systems such as sensors and actuators, end users, data owners but also service providers need strong mechanisms for reliability and trust. Users and residents of the system will require fine-grained access and data privacy policies they want to enforce. For instance, a user might be willing to share location information with family and friends and make the information available in aggregated form for improvement of the public transport. But the same user might not want the information to be used by other 3rd-party service providers. New applications and synergies are possible if the data is shared between multiple domains. However, several challenges need to be overcome to make this possible. Creating a platform for sharing IoT-type of data is per se a huge challenge.

5.1.2 Risks to a Smart City IoT Platform

We predict that smart city data will eventually be stored in the cloud and employ cloud computing techniques, due to the high scalability of resources and computing performance and reduced cost in maintenance and operation. In this case, the smart city management system inherits also the security and privacy risks of cloud computing, for instance the compromise of cloud servers or data abuse by insider attacks. Additionally the Smart Cities infrastructure

is also interacting with sensors and actuators in order to gather data and control critical infrastructure functions. This clearly requires to authenticate and authorize the access and to provide trusted information in a secure and privacy-preserving way.

These examples and developments show the importance of security, privacy and trust in smart city applications. The actual damages caused by possible threats can range from small interferences in the system to personal losses/exposure of private information. With more information and management and control the smart city assets being available over ICT networks, the risk and impact of security or privacy threats is foreseen to be increasing and can have profound and serious consequences for the community.

A smart city infrastructure, as pictured above, is exposed to several risks such as attacks on the control infrastructure, poisoning of data, and leakage of confidential data. SMARTIE will focus on challenges that concern privacy, security and trust of the information available in the smart city. An attacker can simultaneously attack on multiple layers:

- Manipulate the sensor measurements to infiltrate the system with wrong data, e.g. to cause certain actuations
- Attack the sensors and actuators physically to obtain credentials
- Attack or impersonate network components to act as a man-in-the-middle
- Obtain sensitive data or cause actuation by attacking the sharing platform with forged or malicious requests

Standard network security tools such as firewalls, monitoring or typically access control will not suffice to prevent such sophisticated attacks due to the distributed nature of the IoT and the problem of defining/finding trusted parties. It is essential that security is built into the infrastructure rather than being added as an extra plug-ins. An effective protection approach is to have security in depth, where data and services are protected by several independent systems. The challenge will be to design solutions where no single server has significant power to control the infrastructure or to access significant amounts of data.

5.2 First Steps Towards a Secure Platform

Past and current projects, such as UbiSec&Sense, SENSEI, WSAN4CIP provide already some solutions on which a platform as outlined above can build.

We present in this section certain components, which can be used as building blocks, but also components that need further development to be suitable for the type of platform SMARTIE aims for.

5.2.1 Trust and Quality-of-Information in an Open Heterogeneous Network

In SMARTIE and in other IoT systems, systems belonging to different owners need to cooperate. Such a cooperating system can be denoted as a system of systems (SoS). It is an entity composed of independent systems that are combined together in order to interact and provide a given service, which cannot be provided by the individual systems when not cooperating. The major properties of SoS especially for application fields as those intended in the SMARTIE project are dependability, security and privacy. Dependability comprises the following attributes:

- Availability — readiness for correct service
- Reliability — continuity of correct service
- Safety — absence of catastrophic consequences on the system user and its environment
- Integrity — lack of inappropriate system alternations
- Maintainability — ability to undergo updates and repairs

During the last years, the idea that security is needed to ensure real dependability has gained a certain level of acceptance and incidents such as the Stuxnet worm have demonstrated this pretty clear. The main aspects of security are confidentiality (absence of unauthorized disclosure of information), integrity, (the prevention of unauthorized modification or deletion of information) and availability for authorized actions.

All systems within a SoS have their own life, can work without interaction with other systems and are managed by different authorities. To ensure the appropriate cooperation and desired level of dependability and security within the SoS, a SoS management layer has to be designed and developed.

There is a limited theory on how to SoS should be managed [19]. The authors present five characteristics that give possible representation of fundamental building blocks for realizing and managing SoS.

- Autonomy — the ability to make independent choices — the SoS has a higher purpose than any of its constituent systems, independently or additively.
- Belonging — happiness found in a secure relationship — systems may need to undergo some changes to be part of SoS.
- Connectivity — the ability of system to link with other systems — systems are heterogeneous and unlikely to conform to a priori connectivity protocols and the SoS relies on effective connectivity in dynamic operations.
- Diversity — distinct elements in a group — SoS can achieve its purposes by leveraging the diversity of its constituent systems.
- Emergence — new properties appear in the course of development or evolution — SoS has dynamic boundaries, which are always clearly defined, SoS should be capable of developing an emergence culture with enhanced agility and adaptability.

SoS is often viewed as a network in the literature [20]. For management of SoS the "best practices" based on ISO standard ISO/IEC 7498 principles of network management should be used. The ISO defines terminologies, structure, activities for management of IT networks. These principles have been developed based on a systematic approach and thus, can be considered as guideline for the description of other kinds of networks as well. Since we are mainly concerned with heterogeneous groups of devices/services we will call such a SoS a Federation of Systems (FoS).

The need of cooperation in a Federation of Systems requires that the individual systems within FoS have to be trustworthy, and that there is a minimal level of trust between the involved systems. The transitive trust can be used to extend trusted relationship within the group. Kamvar et al. [21] present a reputation system for P2P that aggregates the local trust values of all of the users in a natural manner, with minimal overhead in terms of message complexity. The approach is based on the notion of transitive trust. The idea of transitive trust leads to a system which computes a global trust value for a peer by calculating the left principal eigenvector of a matrix of normalized local trust values. The non-transitive trust and reputation management scheme for wireless sensor networks is presented by Boukerch et al. [22] The approach uses localized trust and reputation management strategy, hence

avoiding network-wide flooding. Each node in the network is able to establish a trust value with other interacting entities.

FAIR (fuzzy-based aggregation providing in-network resilience) [43] is an example how trust can be established and maintained at least between a base station and sensor node in the field. The strength of FAIR is the compatibility with the aggregation hierarchy that makes FAIR well suitable for medium size or large sensor networks. In a smart city scenario, smaller sets of sensors are more likely and we present a variant for trusted Quality of Information (QoI) computation that is particularly well-suited for small unattended networks [44].

The variant is based on a two-step *aggregate-and-confirm* approach. There are three roles pseudo-randomly distributed among the nodes at the beginning of each epoch: the Aggregator Node, the Normal Nodes and the Storage Nodes. The protocol consists of two message rounds, where each message is authenticated and broadcasted:

(1) Periodically, the aggregator node triggers the network to start an aggregation process; each node senses the environment and sends back its measurement.
(2) The aggregator node collects all the values, removes the outliers and computes the aggregate, which consists of the result and a measure of precision. This precision expresses the dispersion of the "genuine" data set. Based on this tuple, each node checks that the result is correct by comparing it with its own measurement and outputs a confirmation digest, encrypted with a pairwise key shared with the base station. Those confirmations are collected and stored by the storage nodes, which keep them for the base station.

Figure 5.2 gives an overview on those two protocol rounds.

The base station does not play any role in the aggregation process; it just retrieves the aggregated results and delivers it to the end user. To do so, the base station authenticated broadcasts to the network the epoch desired. Every node that was a storage node at this epoch and recorded the result sends it back together with the precision and the list of confirmation messages. Thanks to these two parameters, the base station can extract a measure of the Quality of Information (QoI) in order to evaluate the quality of the aggregation process.

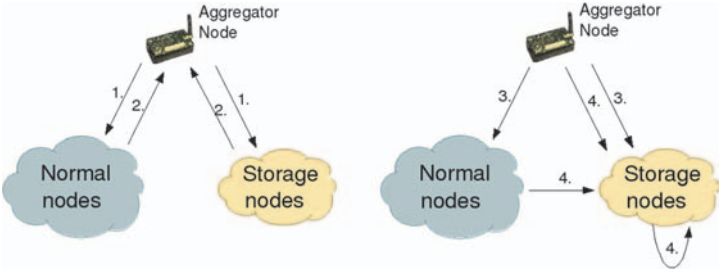

Fig. 5.2 General overview of the protocol: 1. AN triggers the network 2. Network sends back measurements 3. AN aggregates data and send back the tuple [result; precision] 4. Every node checks the result and sends a confirmation message to the SN.

5.2.2 Privacy-preserving Sharing of IoT Data

To the large extent, the IoT data may be of personal nature and therefore it is important to protect it from unauthorised entities accessing it. Privacy is one of the most sensitive subjects in any discussion of IoT protection [23].

Therefore, data privacy is one of the crucial aspects of IoT. The amount of data generated by IoT will be huge. Single pieces of information, i.e., single measurements, in most cases do not represent a significant threat for the owners of IoT devices (temperature at a location, even heart rate of a person at a given moment). However, given that the devices are generating data continuously, it is obvious that unauthorized access to such wealth of data can cause significant problems and can be used to harm the owners of the data (and possibly others, depending on the context of the data). Therefore, it is of paramount importance to protect access to IoT data. On the other hand, the power of IoT lies in the ability to share data, combine different inputs, process it and create additional value. Hence, it is equally important to enable access to data generated by other IoT devices, while preventing the use of data in un-authorized or undesired ways.

The existing initiatives such as FI-WARE [24] address the privacy issue within the Optional Security Service Enabler [25]. The issue of privacy is concerned with authorization and authentication mechanisms. This includes a policy language to define which attributes (roles, identity, etc.) and credentials are requested to grant access to resources. It includes a (data handling) policy language that defines how the requested data (attributes and credentials) is handled and to whom it is passed on. Finally, it includes the means to release

and verify such attributes and credentials. It is also important to consider the mechanisms enabling the protection of information based on encryption algorithms within the secure storage. In terms of the privacy policy implementation, one of the viable solutions is privacy by design, in which users would have the tools they need to manage their own data [26].

The fundamental privacy mechanisms lie in the intelligent data management so that only the required data is collected. Detecting the redundancy, data is anonymised at the earliest possible stage and then deleted at the earliest convenience. Furthermore, the processing of collected data will have to be minimised according to a strict set of rules so that it cannot be re-used. The proposed approach will define such methodology together with the mechanisms for the secure storage based on efficient cryptographic algorithms suited for the resource constrained environments.

Misconceptions of what "personally identifiable information" is have originated multiple privacy scandals over the last years. Naively anonymised data that rely on the fallacious distinction between "identifying" and "non-identifying" attributes are vulnerable to re-identification attacks. Notable examples of supposedly anonymised data release which led to lawsuits in the US are the AOL search queries and the Netflix Prize dataset. While some attributes can be identifying by themselves any attribute can be identifying in combination with others. For example: zip code, sex and birth date combined uniquely identify 87% of the US population [27].

Information disclosure access control must be aware of metrics drawn from data analysis to assess the true risks of privacy breaches. In order to do that, concepts like K-Anonymity and Differential Privacy will be used.

5.2.3 Minimal Disclosure

Individuals wish to control their personal information in the online domain, especially as more and more sensors are available that could be linked to the user in order to generate data. Organisations that are responsible for handling the information of individuals, seem to be minimally concerned with this wish, as can be seen from the large number of severe data leaks during the past years. One guiding principle, data minimisation, is hardly ever practiced and almost never enforced, which leads to very limited user empowerment with respect to privacy. On the other hand, the service providers which rely on the personal

data of their users are asking for more accurate and detailed information, preferably authenticated by a trusted party such as the government.

Three features of privacy-friendly credentials are informally described in NSTIC [28] documents:

(1) Issuance of a credential cannot be linked to a use, or "show," of the credential even if the issuer and the relying party share information, except as permitted by the attributes certified by the issuer and shown to the relying party.
(2) Two shows of the same credential to the same or different relying parties cannot be linked together, even if the relying parties share information.
(3) The user agent can disclose partial information about the attributes asserted by a credential. For example, it can prove that the user if over 21 years of age based on a birthdate attribute, without disclosing the birthdate itself.

Several technologies like U-Prove [29] and IdeMiX have been developed in order to support this need in order to reduce the information to be disclosed.

5.2.4 Secure Authentication and Access Control in Constrained Devices

Embedded systems and especially wireless sensor nodes can be easily attacked. This is due to the fact that they are normally unprotected by cryptographic means. This is due to the fact that both types of devices suffer from severe resource constraints e.g. energy resources and processing power so that standard cryptographic approaches cannot be applied. Thus there is a necessity of development of the lightweight cryptographic solutions, which take the above mentioned constraints into consideration and are able to ensure the needed level of the security.

State of the Art: There are several lightweight security approaches designed for wireless sensor networks. The SPINS [12] protocols encompass authenticated and confidential communication, and authenticated broadcast. [13] uses asymmetric cryptographic schemes to exchange secret session keys between nodes and symmetric crypto approaches for data encryption. The approach presented in [14] provides authentication and authorization of sensor nodes,

a simple but secure key exchange scheme, and a secure defense mechanism against anomalies and intrusions. In addition it supports confidentiality of data and usage of both symmetric and asymmetric schemes. In [15] the authors present LiSP: a lightweight security protocol, which supports all security attributes, but at a high level of power consumption when compared to the protocols described in [14]. The lightweight security approach presented in [16] is based on the RC4 stream cipher. It provides data confidentiality, data authentication, data integrity, and data freshness with low overhead and simple operation. In [17] the authors propose a lightweight security approach based on modification of elliptic curves cryptography. The reduction of the length of the security parameters influences the security level but also helps to save the energy needed for computation and communication. A similar approach is followed in [18]. However, the RSA with limited lifetime is still too expensive for WSNs due to the large size of the messages (>512bit). Such a size of the message requires in most of the WSN platforms packet fragmentation what makes the communication expensive and complicated.

When dealing with access control for IoT, the first considered approach consists in the potential applicability of existing key management mechanisms widely used in Internet that allows performing mutual authentication between two entities and the establishment of keying material used to create a secure communication channel. Nevertheless, due to the computational and power restrictions that must be satisfied in IoT networks, existing mechanisms [30] are not applicable for controlling the access to services offered by IoT networks. For example, while public key cryptography solutions demand high computational capabilities, schemes based on pre-shared keys are not applicable since they would require the pre-establishment of symmetric keys between an IoT device with every Internet host.

For this reason, in the literature we can find different works proposing alternative solutions [31, 32] to cope with the access control problem in IoT networks. For example, one of the earliest works in this area is developed by Benenson et al. [33] where a cooperative access control solution is defined. In this work, user authentication is performed by collaboration of a certain group of IoT nodes. Despite this scheme is carefully oriented to minimize the computation overhead in IoT devices, it increases communication overhead. Following this initial contribution, different access control solutions have been

proposed for IoT networks. Depending on the employed scheme, we can distinguish between public key cryptography (PKC) and shared key cryptography (SKC) based solutions.

On the one hand, PKC schemes [34–38] are based on Elliptic Curve Cryptography (ECC) in order to reduce the computational requirements on IoT nodes. The different schemes vary on the approach used to implement the ECC based authentication. For example, while some solutions require a Key Distribution Centre to be available all the time, others develop a certificate-based local authentication. However, these proposals suffer from requiring high times to conduct user authentication (in some cases times are greater than 10 seconds).

On the other hand, SKC schemes [39–41] propose the user authentication based on symmetric key cryptography algorithms, which are more efficient than public key schemes. The use of these solutions requires both users and IoT nodes to share a secret key that will be used to carry out mutual authentication before granting the user access to the service offered by the IoT nodes. Compared to PKC, SKC schemes require lower computation and capabilities. Nevertheless, these schemes present serious scalability problems since they require the pre-establishment and pre-distribution of keying material.

In summary, we observe that existing access control solutions for services implemented within IoT networks do not offer a proper solution for future IoT. Furthermore, PKC schemes based on ECC favour scalability [42] given that they do not require the pre-establishment and pre-distribution of keying material. Nevertheless, SKC schemes are more advantageous in terms of computational efficiency.

5.3 Smartie Approach

SMARTIE will design and build a data-centring information sharing platform in which information will be accessed through an information service layer operating above heterogeneous network devices and data sources and provide services to diverse applications in a transparent manner. It is crucial for the approach that all the layers involve appropriate mechanisms to protect the data already at the perception layer as well as at the layers on top of it. These mechanisms shall cooperate in order to provide a cross-layer holistic approach.

SMARTIE will focus on key innovations that strengthen security, privacy and trust at different IoT Layers as depicted in the following table:

IoT layers	Security requirements
Applications (Intelligent Transportation, Smart Energy, Public Safety, Utilities, Service Providers, etc.)	• Authentication, Authorisation, Assurance; • Privacy Protection and Policy Management; • Secure Computation; • Application-specific Data Minimisation; • Discovery of Information Sources
Information Services (In-network Data Processing, Data aggregation, Cloud Computing, etc.)	• Cryptographic Data Storage; • Protected Data Management and Handling (Search, Aggregation, Correlation, Computation);
Network (Networking infrastructure and Network-level protocols.)	• Communication & Connectivity Security; • Secure Sensor/Cloud Interaction; • Cross-domain Data Security Handling
Smart Objects (Sensors for data collection, Actuators)	• Data Format and Structures; • Trust Anchors and Attestation; • Access Control to Nodes • Lightweight Encryption

5.3.1 Adaptation and Deployment

In order to demonstrate the advantages and potentially of our approach, we envisage the following application areas for deploying the project architecture.

5.3.1.1 Smart Transportation

Smart City Objectives

- Improving the management of the public transportation networks to foster greater use of sustainable transport modes and to provide time and cost benefits to travellers.

- Involving user smartphones in order to include additional information related to their travels.
- Improving the management of individual motor car traffic, to reduce travelling time in the town, improve traffic flow and reduce fine dust pollution.
- Extending traffic control systems with mobile traffic control systems to react fast on abnormal situations, planned ones (e.g. road reconstruction) and also unplanned ones (e.g. accidents).
- Exploiting heterogeneous wireless sensor networks placed on public transport vehicles and in the environment (streets etc.) e.g. stationary traffic sensors/actuators placed at cruces of the transportation network.

Usage

- Public transportation companies monitor the current demand of travellers for public transportation for certain routes and optimise the number of vehicles to match the demand. They also monitor location of all public vehicles.
- Travel plan component located on the cloud infrastructure calculates the best routing option for the traveller taking into account the traveller location, expected arrival times and current traffic conditions. This information is then forwarded to the associated smartphone application and presented to the traveller.
- City traffic authorities monitor the current traffic conditions:
    - To optimise the traffic lights in order to achieve better traffic flow.
    - To adapt speed limitation signs.
    - To indicate detours in case of road re-construction, accidents or other emergency situations.
- The required adaptation of the individual car traffic is then indicated via adapted traffic light switching, updated electronic traffic sign, etc.

Security and Privacy Challenges

- Information related to location of public vehicles should be accessible to system users according to the access policy and privacy rules.
- All data exchange between the sensor, actuators and backend server should be implemented in a secure manner.
- All the data related to the travellers' location and activity should be considered private, and it should be treated according to the privacy rules.
- Integration systems owned by different parties such as public authorities and private companies providing telematics services.

5.3.1.2 Smart campus

Smart City Objectives

- Monitoring energy efficient in the campus considering energy consumption and energy generation.
- Evaluating real-time behaviour of systems jointly acting as a sustainable ecosystem.
- Providing the user capability to interact with the system to facilitate the improvement of the energy efficiency.

Usage

- Energy Supervisor entity will be able to collect from the different sources: information in real time about building consumption and energy generation from the different entities involved (photovoltaic generators).
- Energy Monitoring entity will collect data from the sensors being deployed and also data aggregated and summarized about the different energy producers to take decisions over different actuators involved in the system.
- Energy Producer will provide data aggregated to the Entity Monitoring based on the agreement established and will provide more detail data to the Energy Supervisor as main regulator.

- User will provide in certain situations their positions and presence information to the Energy Monitoring entity by means of the sensor within the building or light-street pathways.

Security and Privacy Challenges

- Access to the data of the sensor should be controlled based on access control and privacy rules. Hence only certain services of the entity monitoring could read or act over them especially in the case the monitoring entity is a third party.
- The exchange will require mechanisms including data protection and integrity in the transfer between the different parties.
- Scalable and secure management protocol which lets the verification and authentication of new sensors deployed and ensure the extension of the trust domain to new devices in the deployment environment.
- Entities are actually restricted to use the data based on the national protection data law. They will like to explore how to reuse the data and possible being able to share to third parties but also controlling what can be shared based on legislation.
- Data exchange between entities needs to follow data minimization principles and allow traceability.
- User data information exchange could be in some case anonymous and in other case could be needed some control over the distribution of data.

5.4 Conclusion

The Internet of the Future will be a cluster of heterogeneous current and future infrastructures (networks, services, data, virtual entities, etc.) and of usages with mainly decentralized security and trust functions. The emergence of sensing and actuating devices, the proliferation of user-generated content and nascent (Internet-only) services delivery create the need to address trust and security functions adequately.

The idea of the IoT brings new challenges regarding security and in consequence also for privacy, trust and reliability. The major issues are:

- Many devices are no longer protected by well-known mechanisms such as firewalls and can be attacked via the wireless channel directly. In addition devices can be stolen and analysed by attackers to reveal their key material.
- Combining data from different sources is the other major issue since there is no trust relationship between data providers and data consumers at least not from the very beginning.
- Secure exchange of data is required between IoT devices and consumers of their information.

A lot of research effort was put in the protection of wireless sensor networks that might be thought of one of the data sources, but the integration of wireless sensors into a heterogeneous service architecture is still an open issue.

Contrary to these mechanisms developed through history, current trends in the Internet lead to implementation of security and trust by *ex-ante* automatic access controls and technical reliance on secrecy. However, history teaches us to consider setting emphasis on usage rules rather than access rules or collection rules, and rely on the principle of transparency, accountability and enforcement in order to build trust in our Internet society.

SMARTIE solutions will provide a set of innovations and enhancements to address the challenges imposed by the application domains.

References

[1] Seshadri, A., Luk, M., Perrig, A., van Doorn, L., and Khosla, P.SCUBA: Secure code update by attestation in sensor networks. InWiSe '06: Proceedings of the 5th ACM workshop on Wireless security (2006), ACM.

[2] Aurelien Francillon, Claudio Soriente, Daniele Perito and Claude Castelluccia: On the Difficulty of software based attestation of embedded devices. ACM Conference on Computer and Communications Security (CCS), November 2009

[3] Benjamin Vetter, Dirk Westhoff: Code Attestation with Compressed Instruction Code. IICS 2011: 170–181

[4] Trusted Computing Group (TCG) Specification. URL: http://www.trustedcomputing group.org/

[5] Rodrigo Roman, Cristina Alcaraz, Javier Lopez, Nicolas Sklavos, Key management systems for sensor networks in the context of the Internet of Things, Computers & Electrical Engineering, Volume 37, Issue 2, March 2011, Pages 147–159, ISSN 0045–7906.

[6] Butun, I. and Sankar, R. "A brief survey of access control in Wireless Sensor Networks," Consumer Communications and Networking Conference (CCNC), 2011 IEEE , vol., no., pp. 1118–1119, 9–12 Jan. 2011.

[7] Youssou Faye, Ibrahima Niang, and Thomas Noël. A Survey of Access Control Schemes in Wireless Sensor Networks. WASET, World Academy of Science, Engineering and Technology, 59: 814–823, 2011. Note: Selected paper from the ICWCSN 2011, Int. Conf. on Wireless Communication and Sensor Networks.

[8] Z. Benenson, F. Gartner, and D. Kesdogan, "An algorithmic framework for robust access control in wireless sensor networks," in Wireless Sensor Networks, 2005. Proceedings of the Second European Workshop on, pp. 158–165.

[9] X.H. Le, S. Lee, I. Butun, M. Khalid, and R. Sankar, "An energy efficient access control for sensor networks based on elliptic curve cryptography," Journal of Communications and Networks, 2009.

[10] H. Wang and Q. Li, "Distributed user access control in sensor networks," Distributed Computing in Sensor Systems, pp. 305–320.

[11] H. Wang, B. Sheng, and Q. Li, "Elliptic curve cryptography-based access control in sensor networks," International Journal of Security and Networks, vol. 1, no. 3, pp. 127–137, 2006.

[12] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, "SPINS: Security protocols for sensor networks", proc. of 7th annual international conference on Mobile computing and networking, Rome, Italy, Aug 2001, pp. 188–189.

[13] Chris Karlof, Naveen Sastry, and David Wagner, "TinySec: a link layer security architecture for wireless sensor networks", Proc. of the 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA, Nov 2004, pp. 162–175.

[14] Riaz A. Shaikh, Sungyoung Lee, M. A. U. Khan and Young Jae Song, "LSec: Lightweight Security Protocol for Distributed Wireless Sensor Networks", proceedings of the of 11th IFIP Conference on Personal Wireless Communications (PWC 2006), LNCS vol. 4217, Spain, Sep 2006, pp. 367–377.

[15] Taejoon Park, and Kang G. Shin, "LiSP: A Lightweight Security Protocol for Wireless Sensor Networks", ACM Transactions on Embedded Computing Systems, vol. 3(3), Aug 2004, pp. 634–660.

[16] Chang N., Zhang Qian Yu, Cungang Yang, A Lightweight Security Protocol for Wireless Sensor Networks, In Proceedings of the International Workshop on Telecommunications-IWT/07

[17] A. Sojka, K. Piotrowski, and P. Langendoerfer, ShortECC: a Lightweight Security Approach for Wireless Sensor Networks, Proc. INSTICC International Conference on Security and Cryptography, SECRYPT, 2010

[18] Chae Hoon Lim, Practical Broadcast Authentication Using Short-Lived Signatures in WSNs, Information Security Applications, Lecture Notes in Computer Science, 2009, Volume 5932/2009, 366–383.

[19] J. Boardman, B. Sauser, Taking Hold of System of Systems Management. Engineering Management Journal, December 2008

[20] Mo Mansouri, Alex Gorod, Thomas H. Wakeman, Brian Sauser. Maritime Transportation System of Systems management framework: a System of Systems Engineering approach. International Journal of Ocean Systems Management (IJOSM), Vol. 1, No. 2, 2009.

[21] S. D. Kamvar, M. T. Schlosser, H. Garcia-Molina. The Eigentrust algorithm for reputation management in P2P networks, in: Proc. 12th Int'l World Wide Web Conf., Budapest, Hungary, 2003, pp. 640–651.

[22] A. Boukerch, L. Xu, K. El Khatib. Trust-based security for wireless ad hoc and sensor networks. Comput. Commun., Vol. 30, No. 11–12. (2007), pp. 2413–2427.

[23] Securing the Internet of Things, Rodrigo Roman, Pablo Najera, and Javier Lopez, University of Malaga, SpainIEEE Computer, vol. 44, no. 9, pp. 51–58, September 2011.

[24] FI-WARE platform, http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php

[25] FI-WARE Security, http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FI-WARE_Security#Optional_Security_Service_Enabler

[26] Privacy Implications of the Internet of Things, Ivan Gudymenko, Katrin Borcea-Ptzmann, and Katja Tietze, Dresden University of Technology, Department of Computer Science, Chair of Privacy and Data Security, 2011.

[27] L. Sweeney, Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000.

[28] The White House. National Strategy for Trusted Identities in Cyberspace. April 2011. Available at http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

[29] Christian Paquin. U-Prove Technology Overview V1.1 Draft Revision 1. February 2011. Specifications and Documentation page, which itself is available at http://www.microsoft.com/u-prove.

[30] Rodrigo Roman, Cristina Alcaraz, Javier Lopez, Nicolas Sklavos, Key management systems for sensor networks in the context of the Internet of Things, Computers & Electrical Engineering, Volume 37, Issue 2, March 2011, Pages 147–159, ISSN 0045-7906.

[31] Butun, I. and Sankar, R. "A brief survey of access control in Wireless Sensor Networks," Consumer Communications and Networking Conference (CCNC), 2011 IEEE , vol., no., pp. 1118–1119, 9–12 Jan. 2011.

[32] Youssou Faye, Ibrahima Niang, and Thomas Noël. A Survey of Access Control Schemes in Wireless Sensor Networks. WASET, World Academy of Science, Engineering and Technology, 59: 814–823, 2011. Note: Selected paper from the ICWCSN 2011, Int. Conf. on Wireless Communication and Sensor Networks.

[33] Z. Benenson, F. Gartner, and D. Kesdogan, "An algorithmic framework for robust access control in wireless sensor networks," in Wireless Sensor Networks, 2005. Proceedings of the Second European Workshop on, pp. 158–165.

[34] X. H. Le, S. Lee, I. Butun, M. Khalid, and R. Sankar, "An energy efficient access control for sensor networks based on elliptic curve cryptography," Journal of Communications and Networks, 2009.

[35] H. Wang and Q. Li, "Distributed user access control in sensor networks," Distributed Computing in Sensor Systems, pp. 305–320.

[36] H. Wang, B. Sheng, and Q. Li, "Elliptic curve cryptography-based access control in sensor networks," International Journal of Security and Networks, vol. 1, no. 3, pp. 127–137, 2006.

[37] Y. Zhou, Y. Zhang, and Y. Fang, "Access control in wireless sensor networks," Ad Hoc Networks, vol. 5, no. 1, pp. 3–13, 2007.
[38] H. F. Huang, "A novel access control protocol for secure sensor networks", Journal of Computer Standards and Interfaces, Elsevier, 2009.
[39] Y. Shen, J. Ma, and Q. Pei, "An access control scheme in wireless sensor networks," in Network and Parallel Computing Workshops, 2007. NPC Workshops. IFIP International Conference on, 2007, pp. 362–367.
[40] K. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks." IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006.
[41] H. Tseng, R. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks." IEEE Global Communications Conference, 2007.
[42] H. Wang, B. Sheng, C. Tan, and Q. Li, "Comparing symmetric-key and public-key based security schemes in sensor networks: A case study of user access control." The 28th International Conference on distributed Computing Systems, ICDCS'08, 2008, pp. 11–18.
[43] Emiliano De Cristofaro, Jens-Matthias Bohli, Dirk Westhoff: FAIR: fuzzy-based aggregation providing in-network resilience for real-time wireless sensor networks. WISEC 2009: pp. 253–260.
[44] Jens-Matthias Bohli, Panos Papadimitratos, Donato Verardi, Dirk Westhoff: Resilient data aggregation for unattended WSNs. LCN 2011: pp. 994–1002

6

A Common Architectural Approach for IoT Empowerment

Alessandro Bassi[1], Raffaele Giaffreda[2], and Panagiotis Vlacheas[3]

[1]*IoT-A project, Bassi Consulting, France.*
[2]*iCore project, CREATE-NET, Italy.*
[3]*iCore project, University of Piraeus, Greece.*

6.1 Introduction

The need of a "lingua franca" for the Internet of Things domain is clearly stated by many, if not all, EU projects running within this domain.

The "Internet of Things — Architecture" [1] project reckons that the past and current developments within this area should be called "Intranet of things". This is because different solutions were developed with a narrow target in mind, resulting in a large number of different means to enable communication between heterogeneous devices. The result is vertical "silo" structures that are not suited for supporting interoperability or further extensions of capabilities. Given this premises, it's rather easy to predict that this balkanisation of efforts is slowing down the developments of economically sustainable solutions. Furthermore, existing solutions do not address any requirements for a global scalability of the future Internet of Things; they provide inappropriate models of governance and fundamentally neglect privacy and security in their design.

Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, 245–257.
© 2013 *River Publishers. All rights reserved.*

Similarly, BUTLER [2] insists on existence of domain-centric smart solutions, and aims at developing a horizontal solution in order to enable the development of secure and smart life applications.

iCore [3] addresses two key issues in the context of IoT, namely how to abstract the technological heterogeneity that derives from the vast amounts of different objects while enhancing reliability and how to consider the views of different users/stakeholders for ensuring proper application provision.

IoT6 [4] aims at exploiting the potential of IPv6 and related standards such as 6LoWPAN and CoAP to overcome current shortcomings and fragmentation of the Internet of Things. Its main challenges and objectives are to research, design and develop a highly scalable IPv6-based Service-Oriented Architecture to achieve interoperability, mobility, cloud computing integration and intelligence distribution among heterogeneous smart things components, applications and services.

The same issue is at the foundations of the iot.est [5] project. They see current implementations of Internet of Things architectures confined to particular application areas and tailored to meet only the limited requirements of their narrow applications. Their take in order to overcome technology and sector boundaries to be able to design and integrate new types of services and generate new business opportunities is a service creation environment that gathers and exploits data and information from sensors and actuators that use different communication technologies/formats.

This list is clearly incomplete, and looking through each and every project belonging to the IERC Cluster it's possible to find a similar analysis, if not the same, The aim towards a solution that helps federating current developments and creating a synergistic environment for the developments of future services and applications is definitely mainstream within the EU-funded projects in the area.

Is this result achievable? With the "cream" of EU research converging on this aim, the answer may seems obvious at first glance. What is more important to see, though, is at what level a convergence can be achieved, and which design choices will make all future developments interoperable.

At times of writing, it seems very unlikely, if not clearly impossible, that a single design pattern will be used for all envisaged applications. The diversity of application domains provide totally different requirements that are solved by a number of different heterogeneous technologies. It is unrealistic to conceive

one-size-fits-all meaningful reference architecture able to implement contrasting needs and specifications. Furthermore, the application domains being so different, different maturities of solutions in industrial and public take-up of IoT development lead to a uneven environment.

Just to make one example, some fields such as manufacturing and logistics have well-established communication and tagging solutions. Business benefits of fully automated processes have been already studied and analysed, and the advantages in terms of asset tracking and supply-chain management are clear. However, the same maturity does not apply for other fields such as domotics, where business synergies between different actors could develop services with clear added-value benefits for the end-users.

While quite logical at this early development stage, this situation needs a clear change in order to foster the necessary advances. As in the networking field, where several communication solutions were developed at an early stage, to leave place to the now universally adopted TCP/IP protocol suite, the emergence of a "common ground" for the IoT domain and the identification of reference architectures will lead to a faster, more focused development, where an exponential increase of IoT-related solutions could take place. These solutions can provide a strategic advantage to world economies, as new business models can leverage emerging technological solutions.

The architectural convergence issue has been clearly identified by the IoT-A project, the flagship EU co-funded project on IoT architectural development.

6.2 Defining a Common Architectural Ground

The IoT-A project aims at extrapolating commonalities and defining an abstraction layer that is common to all IoT-related existing architectures. Therefore, the foundations of its analysis lie on the current state of the art, promoting an evolutionary approach rather than a clean-slate development. This has the major advantage of ensuring backward-compatibility of the model and also the adoption of established, working solutions to various aspects of the IoT.

Following this philosophy, the project collected literally hundreds of IoT-related requirements with the help of end users, organised into a stakeholders group. Once this work was done, it became clear that a single architectural

pattern was unable to satisfy all the possibly contrasting expectations, and that only the abstraction level of a reference model could provide the common ground for any single IoT-based application.

6.2.1 The IoT-A Reference Model

This **IoT Reference Model** provides the highest abstraction level for the definition of the IoT-A Architectural Reference Model. It promotes a common understanding of the IoT domain. The IoT Reference Model is composed by different models that refer to specific aspects of the modeling exercise. In particular, models composing the Reference Model are the IoT Domain Model that describes the generic components of a generic architecture, an IoT Information Model explaining the data semantics typical for an IoT system, and an IoT Communication Model in order to understand specifics about communication between many heterogeneous IoT devices and the Internet as a whole. Furthermore, the functional model and a global security analysis provide two important aspects of the IoT context.

The definition of the IoT Reference Model is conforming to the OASIS reference model definition.

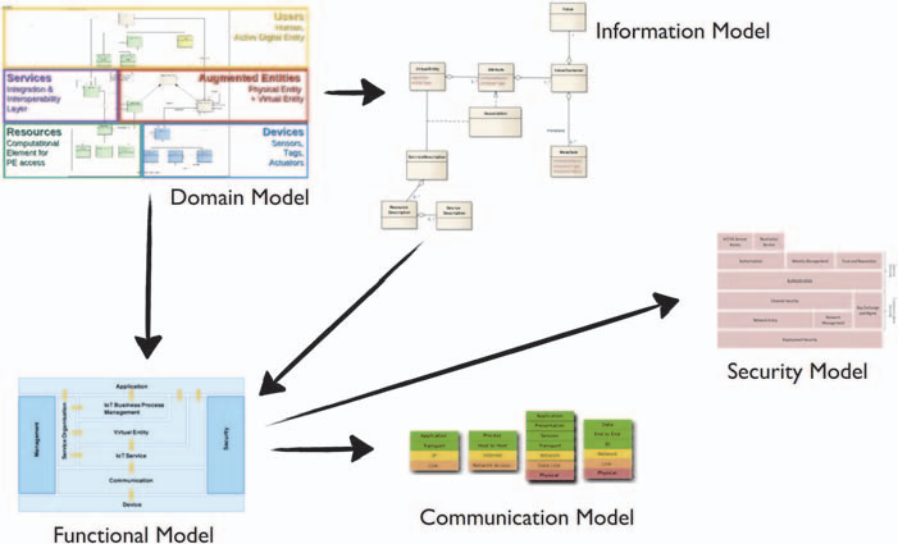

Fig. 6.1 IoT-A Reference Model.

More in particular, the main purpose of a **Domain Model** is to generate a common understanding of the target domain in question, which is of central importance to understand architectural solutions and to evaluate them.

Generically, an abstract IoT scenario can be described as generic user that needs to interact with a physical entity (PE) belonging to the physical world, within this context, a user can be a living creature or any kind of digital artifact, such a service or a software agent.

Physical Entities are represented in the digital world via Virtual Entities, in a one-to-may relationship. The Augmented Entity makes this association explicit, which is the composition of the two. As it enables every day's objects to become part of digital processes, it clearly represents the commonly used concept of "smart device".

In the IoT context, a physical entity is linked with a device, which is able to sense or modify its environment. *Resources* are software components that provide information about or enable the actuation on *Physical Entities*. While Resources are usually heterogeneous, *Services,* defined as the mechanism by which needs and capabilities are brought together, mask the diversity of the underlying levels offering well-defined and standardised interfaces, for interacting with *Physical Entities* and related processes.

The IoT **Information Model** defines the structure in terms of relations and attributes of all the information that is handled in a system on a conceptual level. This includes the modeling of the main concepts for information flow, storage and their relation. The description of the representation of the information and concrete implementations are not part of the IoT Information Model; they can be found in the information view.

The **Functional Model** contains seven longitudinal functionality groups complemented by two transversal functionality groups (Management and Security). These longitudinal groups are: Device, Communication, IoT Service, Service Organisation, Virtual Entity, IoT Business Process Management, and Application. The orthogonal groups provide functionalities that are required by each of the longitudinal groups. The policies governing the transversal groups will not only be applied to the groups themselves, but do also pertain to the longitudinal groups.

The **Communication Model** defines the main communication paradigms for connecting smart objects. It provides a reference communication stack, together with insights about the main interactions among the actors in the

domain model. The communication stack proposed is similar to the ISO OSI 7-layer model for networks, mapping the needed features of the domain model onto communication paradigms. As well, the description of how communication schemes can be applied to different types of networks in IoT belongs to this model.

6.2.2 The IoT-A Reference Architecture

The Reference Model is however too abstract to be used for building directly concrete architectures. In order to implement a compliant IoT solutions, **Reference Architectures** must be defined, describing essential building blocks as well as design choices able to select specific constructs able to deal with converging requirements regarding functionality, performance, deployment and security, to name a few. Interfaces among different technological functional blocks should be standardised, best practices in terms of functionality and information usage need to be provided.

Existing literature provides methodologies for dealing with system architectures (hereafter called Concrete Architectures) based on Views and Perspectives. The way that the IoT-A project illustrates the Reference Architecture (RA) is through a *matrix* that provides clear technological choices in order to develop concrete architectures. To establish the contents of this matrix we need to analyse all possible functionalities, mechanisms and protocols that can be used for building any concrete IoT-related architecture and to show how interconnections could take place between selected design and technological choices. A system architect should then have a tool to make a rational selection of protocols, functional components, and architectural options, needed to build specific IoT systems.

The IoT-A project sees views as a representation of one or more structural aspects of an architecture that illustrates how the architecture addresses one or more concerns held by one or more of its stakeholders.

Viewpoints aggregate several concepts to make the work with views easier. The IEEE Standard 1471 defines viewpoints as follows:

> "A viewpoint is a collection of patterns, templates, and conventions for constructing one type of view. It defines the stakeholders whose concerns are reflected in the viewpoint and the guidelines, principles, and template models for constructing its views."

Some typical examples for viewpoints are Functional, Information, Concurrency, Development, Deployment and Operational viewpoints.

However, architectural decisions often address concerns that are common to more than one view. These concerns are often related to non-functional or quality properties. The approach that the project is following is to define special perspectives to address these aspects of a concrete architecture, emphasising the importance of stakeholder requirements. Therefore we are define a perspective as *a collection of activities, tactics, and guidelines that are used to ensure that a system exhibits a particular set of related quality properties that require consideration across a number of the system's architectural views*, where a quality property is defined as *an externally visible, non-functional property of a system such as performance, security, or scalability*.

A complete description of the IoT-A approach can be found in documents on the IoT-A web site (www.iot-a.eu).

6.3 The iCore Functional Architecture

6.3.1 General Overview

In its most generic sense, the interaction with an iCore system is initiated through a Service Request generated for the purpose of activating data-streams from IoT objects and continuously processing these to support an end-user/ICT application with a set of processes monitoring a situation and producing alerts when particular conditions are met. Such processes, derived from service templates are orchestrated and bound to relevant IoT objects using iCore functionality. This is composed of the three main levels where the bottom one is called Virtual Object (VO) level and is meant to semantically and reliably represent real-world objects, the middle layer is called Composite Virtual Object (CVO) level and expected to provide the means for simple aggregation of VO functionality, whereas the top level, called Service Level (SL) is expected to map availability of underlying CVO/VO features to the needs of end-users and associated IoT applications.

Figure 6.2 shows the iCore architecture at a first level approximation, where a Service Request is transformed via the Service Level functionality into a Service Execution Request, which is then passed to the lower CVO/VO levels for the selection and activation of appropriate objects needed for satisfying

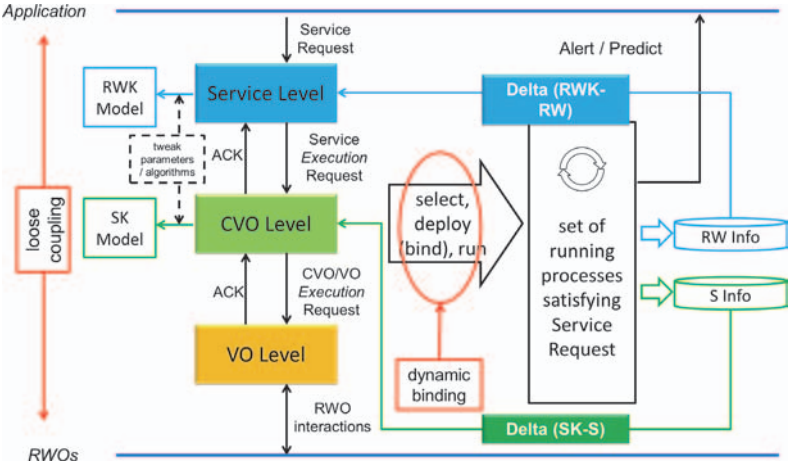

Fig. 6.2 ICore Architecture.

the request. Behind this simple set of processes, iCore value stands in the loose coupling between service requests and actual IoT available objects or a combination of these, which satisfy the request as well as in the ability to select these dynamically, runtime and purposefully through the use of cognitive technologies. This value is reflected also by the ability of iCore system to learn and adapt to changing situations the way it satisfies requests. The figure also shows the rough interactions between the iCore levels cascaded after the Service request, resulting in a set of running processes that is expected to produce runtime notifications and alerts throughout execution.

Besides fulfilling the Service Request needs, iCore is designed to improve IoT systems ability to "grow" and therefore represent Real World Knowledge (RWK) as well as System Knowledge (SK). The first of these abilities is realised within the Service Level where external user feedback or other assessment of accuracy of service behaviour is used to tweak parameters in the selected service template. Within the CVO level similar ability to grow System Knowledge is realised, which helps select or refresh for example the best objects that can fulfil a CVO/VO request. In both cases, the objective is to continuously refine the (RWK/SK) information models therefore minimizing the discrepancy between the way an iCore system can represent the real world and the system itself, for the needs of the requested services and for resource-optimal fulfilment of those by the system. In the remainder of this section we

delve deeper behind the scenes of the iCore interactions and features, describing the first results which lead to the iCore functional architecture.

6.3.2 Actors of the iCore Architecture

The iCore system defines actors in the functional architecture, also corresponding to distinguished business roles (see Figure 6.3 below). The Service Requester is the actor, normally a human user or a software application. The Domain Expert/Knowledge Engineer is an expert of a specific application domain that designs in an iCore specific format (Service Template) how basic services can be built and/or provides base models of a range of specific application or knowledge domains by means of domain ontologies (Real World Knowledge (RWK) Model). The Data Processing Domain Expert/Developer is the developer that designs in a specific format (CVO Template) how basic functions offered by specific VO types that are described in specific format (VO Template) can be combined to build a more complex function. The Device Installer is the user that installs the physical sensor/actuator/resource devices in the iCore system as registered at the iCore VO Level.

Image available in original Version

6.3.3 Functional Blocks and Basic Interfaces Among Them

For the sake of clarity, we split the description of functional blocks in three subsections: Service Level, CVO Level, VO Level.

6.3.3.1 Service Level Functionality

Natural Language Processing (NLP) is the functional block that translates non-technical user human language queries and statements into the formal iCore service request SPARQL query. The Service Request Analysis comprises the Service Analysis block which receives the SPARQL query and asks for the retrieval (through the Intent Recognition) of the current situation in which the query is performed. The Semantic Query Matcher comprises semantic alignment/learning enhancements as a potential pre-processing for the standard SPARQL matching of query to Service Template concept as done in the RDF Rules Inference Engine. The outcome of the RDF Rules Inference Engine is actually a logical mash-up of CVO-selection criteria (i.e. CVO Template names, in its simplest form), called Service Execution Request, which is to be handed over to the CVO Level for service execution. The Service Execution Request is the final outcome of the Service Request Analysis and comprises — apart from CVO-selection criteria — Service Level Agreement (SLA) criteria that express quality demands and cost criteria.

The Service Template Repository contains a semantically query-able collection of Service Templates, as provided in the repository by the Domain Expert/Knowledge Engineer. The Intent Recognition comprises the cognitive functionality that is used to determine what the Intent of the User is and assists in identifying the "Monitoring Goals" (application specific) needed for Situation Detection sub-block of the Situation Awareness block. The User Characterisation comprises the determination of a range of facts concerning a human user, including user context, profile, preferences and policies.

The Situation Awareness block is responsible for the creation of the RWK info, which is then stored in the RWK model. The situational awareness process is generated by a logical sequence of steps/sub-blocks namely (i) Situation Detection (ii) Situation Recognition (iii) Situation Classification and (iv) Situation Projection. Cognition adds the element of intelligence which helps discerning the situation and thereby resulting action. Each of the above sub-blocks follows the cognition cycle in terms of Perception

(Input) — Comprehension (Processing) — Adaptation (Response) tuned to specific goals.

Specific CVOs are devoted to the particular task of observation of events though CVO processing, as particularly meaningful and relevant to the 'situation' that a particular person or service is in. These CVOs are called Situation Observers (SO). The SOs are considered to provide runtime input to the Situation Awareness through the Queried Fast Collector.

The Queried Fast Collector is used to aggregate the subscribed event streams and to deliver the outcome to the Situation Detection of the Situation Awareness, having the latter to create the RWK. The information (about specific RW instances) captured through the event streams is stored in the Real World Information (RWinfo) Database. Finally the Real World Knowledge Model is used for the internal data representation of RWK and we assume that 'knowledge' can be captured in RDF graphs, and so an RWK Model Store can be used to memorise the reflection of the real world's rules of behaviour in the iCore system.

6.3.3.2 CVO Level

The CVO level receives from the Service level a Service Execution Request. The first point of contact in the CVO level is the CVO Management Unit which comprises the CVO Lifecycle Manager an intelligent monitoring unit keeping track of the changing states of the collection of running CVOs. At the time of a Service Execution Request, the lifecycle manager needs to check if CVO instances for a specific CVO template are already running and could be reused, and otherwise needs to instantiate a new CVO through the CVO Factory. When CVOs are used in the context of multiple service execution requests the potentially different service objectives must be coordinated for potential conflict resolution (Coordination functional block). The Performance Management intends to guarantee the proper performance of the CVO Level in terms of satisfying specific Key Performance Indicators (KPIs) thresholds. The Quality Assurance targets mainly at the satisfaction of the SLAs as delivered by the Service Level. Both the Performance Management and the Quality Assurance may trigger reconfiguration actions in order to improve the performance and the quality of service respectively.

CVO Factory: While the CVO Management Unit is more about the execution/runtime aspects of resource management, the CVO factory is

concerned with the production of new or re-instantiation of existing running CVO instances.

- the Approximation and Reuse Opportunity Detection performs a search in order to discover potentially available, relevant CVO instance. If no match is found, then the CVO instance should be created from scratch.
- the CVO Composition Engine will mash up the appropriate VO instances and CVOs to form the complete service graph, ready for execution and therefore must communicate with the VO Level to ask for VO instances of the required VO templates.
- The Orchestration and Workflow Management is one means the iCore system has to further manage the dynamics of the running graphs of CVOs. System Knowledge (SK) based cognition (Learning Mechanisms) can be exploited to identify further optimizations.

The System Knowledge that is built by the Learning Mechanisms is stored in System Knowledge (SK) Model. The CVO Template Repository is a collection of CVO Templates while the CVO Registry contains metadata for each deployed CVO instance, which is preserved for a specific time period. The CVO Container is the actual execution environment of the CVO instances which are monitored and managed by the CVO Management Unit. CVO Container event streams may be aggregated by the Queried Fast Collector bringing new facts, relevant to the RWK, to the Service Level.

As anticipated Situation Observers are specific CVOs that are devoted to the particular task of observation of events though CVO processing, as particularly meaningful and relevant to the 'situation' that a particular person or service is in. iCore ultimately targets leveraging cognition (learning) techniques to identify 'universally relevant'/generic SOs beyond (but using as a starting point the RWK already available in) the explicit observation as auto-decomposable from particular service requests.

6.3.3.3 VO Level

The VO Level, virtualising the sensor (&actuators) data for any service needs receives from the CVO Level a CVO Execution Request which is then passed from the CVO Factory (CVO Composition Engine) towards the VO Management Unit (through the CVO Management Unit). This one, together

with VO Lifecycle Manager, VO Factory/Template Repository/Registry and the Coordination functional blocks have similar roles to their CVO Level counterparts.

The Resource Optimization optimizes by means of cognition the operation of the underlying sensors, actuators and resources e.g. by reducing the energy consumption. The Data Manipulation/Reconciliation takes care of the data management and ensures the quality of the data.

Similarly to its CVO counterpart, the VO Container is the execution environment of the VO instances monitored, controlled and managed by the CVO Management Unit through the VO Management Unit. Each VO comprises two parts: the Front End and the Back End. The Front End is the abstract part of the VO making it interoperable. It comprises the VO template filled with the specific to the VO instance information. The front-end helps also checking the access rights and communicating with the IoT based on IETF protocols on top of IP. The Back End calls Device Manufacturer/vendor provided libraries for communicating with the RWO.

Acknowledgments

The authors would like to acknowledge all the contributors of the deliverable D1.4 of the project IoT-A, in alphabetical order: Martin Bauer (NEC), Mathieu Boussard (ALBLF), Nicola Bui (CFR), Francois Carrez (UniS), Pierpaolo-Giacomin (HEU), Edward Ho (HSG), Christine Jardak (SIEMENS), Jourik De Loof (ALUBE), CarstenMagerkurth (SAP), Stefan Meissner (UniS), Andreas Nettsträter (FhG IML), Alexis Olivereau (CEA), Alexandru Serbanati (CATTID), Matthias Thoma (SAP), Joachim W. Walewski (SIEMENS) Frank Berkers (TNO), Matti Eteläperä (VTT), Darminder Ghataoura (University of Surrey), Stephane Menoret (Thales), Roberto Minerva (Telecom Italia), Septimiu Nechifor (SIEMENS), Abdur Rahim (CREATE-NET), Marc Roelands (Alcatel Lucent) Vera Stavroulaki (UPRC), and Filippo Visintainer (CRF).

References

[1] www.iot-a.eu
[2] www.iot-butler.eu
[3] www.iot-icore.eu
[4] www.iot6.eu
[5] www.ict-iotest.eu

This page intentionally left blank

7

Internet of Things Standardisation — Status, Requirements, Initiatives and Organisations

Patrick Guillemin[1], Friedbert Berens[2], Marco Carugi[3], Marilyn Arndt[4], Latif Ladid[5], George Percivall[6], Bart De Lathouwer[6], Steve Liang[7], Arne Bröring[8], and Pascal Thubert[9]

[1]*ETSI, France.*
[2]*FBConsulting, Luxembourg.*
[3]*ITU-T.*
[4]*Orange, France.*
[5]*University of Luxembourg, IPv6 Forum for IETF, Luxembourg.*
[6]*Open Geospatial Consortium, US.*
[7]*University of Calgary, Canada.*
[8]52°*North, Germany.*
[9]*Cisco, France.*

7.1 Introduction

This section was originally created with IERC (www.internet-of-things-research.eu) stakeholders to link their IoT research, development and innovation activities to international standard organisations, including ETSI, ITU-T, CEN/ISO, CENELEC/IEC, IETF, IEEE, W3C, OASIS, oneM2M and OGC. In 2013 the IERC IoT standard coordinators have asked contributors to focus on latest IoT standardisation issues and to recommend candidate organisations where technical specifications and standards should be developed?

Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, 259–276.
© 2013 *River Publishers. All rights reserved.*

7.1.1 What is Standardisation?

Which definition of standardisation are we using in this chapter?

Standardisation is a voluntary cooperation among industry, consumers, public authorities and other interested parties for the development of technical specifications based on consensus. Standardisation complements market-based competition, typically in order to achieve objectives such as the interoperability of complementary products/services, to agree on test methods and on requirements for safety, health and environmental performance. Standardisation also has a dimension of public interest. Standard makers should be close to standard users/implementers.

7.1.2 What are the Gaps between IoT Standardisation, IoT Research, IoT Development and IoT Innovation?

There are gaps between IoT standardisation and IoT Research, Development and Innovation life cycle. How do IERC stakeholders bridge them?

In order to fill gaps between IoT Research, Development and Innovation and standardisation life cycles (Figure 7.1), IERC encourages the creation of pre-standardisation groups. They allowed to build communities around consensus to develop standards, for example on Semantic Interoperability. Because of many options, IERC has helped to select and coordinate a lot of standards initiatives. IERC is also required to keep IoT Research and Development close to industry innovation and market. How has that been possible?

Industrial workshops have been co-organised with project and the European Commission in order to feed back IoT standardisation activities conducted by industrial stakeholders into EC funded projects. For example ETSI has co-organised workshops on Future Networks, M2M, Cloud, Smart Cities, ITS and RRS. IoT communities also welcomed the organisation of events (like Plugtests/Plugfests, Connectathon, Bake-off) focussing on interoperability testing, coexistence trials and compatibility involving applications or pilots/trial. Next workshops and interoperability "Plugtests/Connectathon" events should focus on IoT performance, optimization, quality (QoS, QoE), trust, safety, privacy, governance and security.

While pre-standardisation like conducted in IRTF/ISOC, ITU-T Focus Group, IEEE-SA Industry Connection Program and ETSI Industry Specification Groups facilitates to bridge the gaps between research and

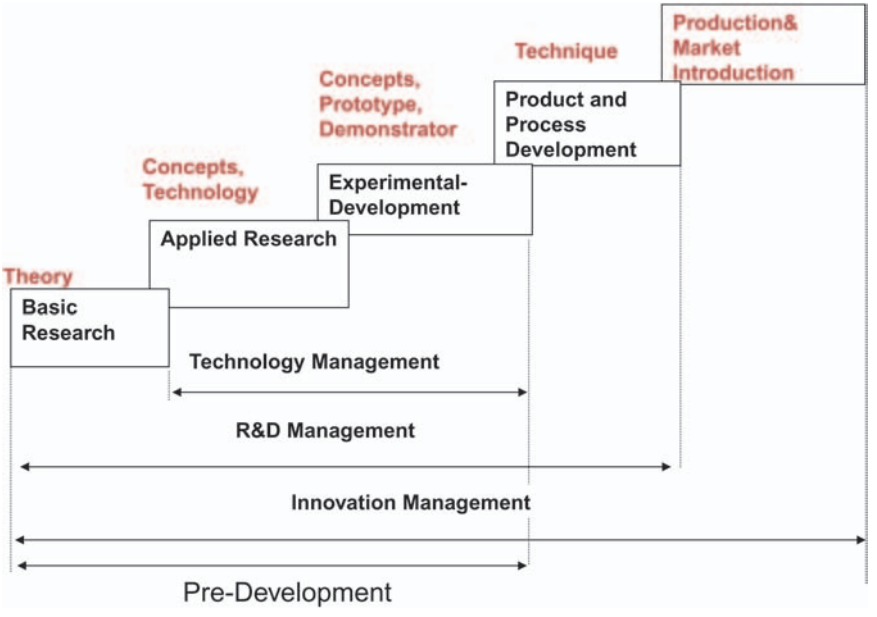

Fig. 7.1 Research, development and innovation life cycle.

standardisation, the on-time creation of Technical Committees (like ETSI TC M2M, TC NTECH) and international Partnership Projects (like ETSI 3GPP and oneM2M) helps to link the international industry with IERC research.

7.1.3 What are Current IoT Requirements?

Without IoT standards, FI-WARE (www.fi-ware.eu) for example would not have been able to successfully provide open "Generic Enablers" for Future Internet/IoT developments in Phase 2 and 3 of FI-PPP (www.fi-ppp.eu). In IERC standardisation coordination meetings the most important IoT requirements for cross-domain standardisation were about cybersecurity, privacy, identification, traceability, anonimization, semantic interoperability, interoperability or coexistence testing, performance characterization and scalability, auto-configuration, discovery, self-configuration, service robustness and resilience. Future standards adopters must be the standards makers. They know best what they need to drive their business. There is a risk that standards are not used if these two kinds of actors are different. An incentive to facilitate

common early standard development is to include pre-standardisation "work packages" within research projects proposals. However, there could be a lack of industrial involvement. This is why IERC tries to be a central reference for pre-standardisation activities of EC IoT research projects to increase overall efficiency and raise mutual awareness, defragment and synergize in one unique place important information for stakeholders: Industry, Standard Development Organisations (SDOs), European Commission (EC). Before enforcing EC priorities using EU Regulation (Communications, Recommendations, Mandates or Directives) the EU funded programs are giving indication to proposers on EC priorities and domains, SDO/pre-standardisation activities to use, other ongoing projects, actions and deliverables to coordinate with. The IERC exists exactly for that, it allows exchanges between IERC, other EC clusters and projects like Future Networks, Cloud, FI-PPP, and FIA. This helps to detect standards gaps and overlaps and to link with regulation.

7.2 M2M Service Layer Standardisation

7.2.1 M2M Service Layer in IoT

In order to be able to move from a vertical only approach to an integrated horizontal approach a standardisation of generally used service for the communication between devices and between devices and applications is essential.

Only by a world-wide standardisation on a protocol layer between transport and application, a smooth integration of the diverge underlying communication technologies on the lower layers can be guaranteed. Already in a single vertical application domain a large variety of different communication standards exist and will exist in the future. It is not realistic to assume that a single standard on the lower protocol layers can be defined. Thus the integrating mechanism of the future horizontally integrated Internet-of-Things need to be a common cross vertical service layer. This service layer has to provide a set of general services to the applications at all components of the overall architecture from the devices level over the gateways to the network domain. A future worldwide standardised M2M service layer including definitions of interworking with existing underlying standards like 3GPP [5] or iPv6 on the WAN side, ZigBee or KNX on the M2M area side [4] and a clear definition of application interfaces will open up a complete new business opportunities for existing players and more important for new players. The heterogeneous

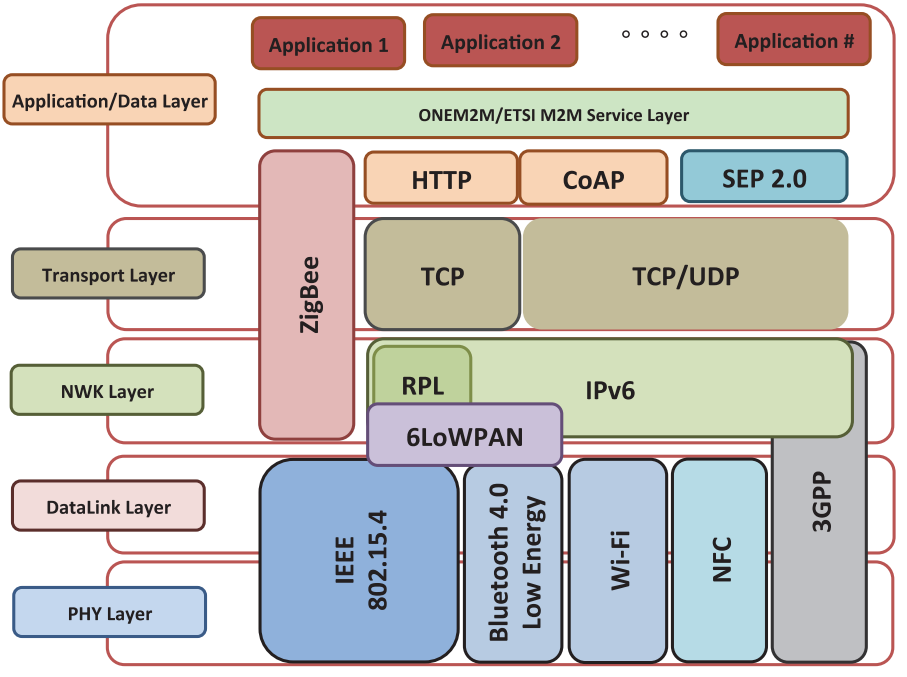

Fig. 7.2 Heterogeneous standards environment in IoT.

standards environment is depicted in Figure 7.2. As such this horizontally integrated service layer can be seen as the operational system of the future IoT providing a set of commonly required services to a broad range of applications and underlying communication technologies.

7.2.2 Cross Vertical M2M Service Layer Standardisation

The main tasks in the standardisation activities will be the integration of different vertical including their communication standards and the definition of clear interoperability methods.

Here a worldwide standardised service layer for M2M type of communication will provide a framework for the integration of the different communication technologies deployed in the field of IoT. This M2M service layer will provide the needed services like data transport, security, devices management and device discovery [1] in a harmonized manner across a multitude of vertical domains to the application layer. These services will be independent from the

underlying communication infrastructure and the deployed standards. In addition to these basic services across vertical semantic support should be included into the service layer capabilities allowing the different vertical domains to represent their semantic information in a horizontal framework.

In recent years several standardisation activities towards a horizontal service layer approach have been started by different standardisation organizations (SDO) world-wide. Here the activities at TIA in the TIA-50 group (M2M Smart Device Communication) in the USA, CCSA TC10 in China and the activities in the ETSI TC M2M group in Europe should be explicitly mentioned. The European activities in ETSI in the scope of ETSI TC M2M can be seen as the most advanced set of horizontal M2M service layer specification with a first release of the standard at the end of 2011 [1, 2, 3] and a finalization of Release 2 during 2013. Figure 7.3 gives an overview over the different communication domains and objects in the ETSI M2M solution.

Since the creation of oneM2M PP the ETSI technical work on the core M2M service layer will be moved to oneM2M. The scope of the ETSI M2M activity will evolve towards a broader handling and coordination of IoT related standardisation topics and the interfacing between oneM2M and the European

Image available in original Version

(*Source*: ETSI TC M2M).

organisations (EU Mandates, EU regulation) and EU research projects including the IERC cluster.

The CCSA (http://www.ccsa.org.cn/) in China standard defines a simple service layer with main drawback in the security and privacy domain. Based on these developments an operational M2M service layer called WMMP exists and is being used by China Mobile. This service layer has a limited capability and can be seen as light version of a service layer.

The TIA-50 (http://www.tiaonline.org/) activities in USA have lead to an initial set of standards with the main focus on the devices and gateway side with a clear lack of network support. Just recently corresponding activities have been launched in this group.

In 2010 the major players in the field have identified the need of a world-wide harmonized standard for the service layer for an M2M like communication. Based on this clear requirement the leading SDO in Europe (ETSI), USA (TIA, ATIS), China (CCSA), Korea (TTA) and Japan (TTC, ARIB) have created a world-wide partnership project called oneM2M (http://www.onem2m.org/) which is operational and in place since September 2012. Participation in the partnership project is open for the individual SDO member companies and institutions. The participating SDOs intend to transfer all standardisation activities in the scope of M2M service layer to the oneM2M PP and with that stop their individual activities in the domain. Regional tasks and adaptation of the standards toward the regional regulation will stay in the responsibility of the regional SDOs. In the near future the participation to the oneM2M will be opened to other standards group and fora like the Broad Band Forum (BBF) and the Continua Health Alliance as representatives of specific vertical application domains.

oneM2M is planning a first release of a set of standards for a service layer for the beginning of 2014. The requirements are based on the use cases developed in the different SDO's and will lead to a world-wide M2M service layer solution.

7.2.3 Business Opportunities and Future Markets

Existing service layer are mainly focused on a single vertical solution like the smart home or smart office environments.

These proprietary solutions are provided by companies like iControl (http://www.icontrol.com/) and nPhase (http://www.nphase.com/) with a

limited possibility to extend the solution and to adapt it to new application areas and domains.

An open world-wide standard M2M service layer based on the future oneM2M standard will open up the possibility for a broad range of companies and players to enter the business field with different sets of possible business models. A broad range of business models and solutions can be envisaged.

In an initial deployment phase companies can provide the software and the required services for the implementation of a full M2M network for the service providing companies and the device manufacturers. The available open application interfaces in the different component of the M2M architecture (device, gateway, network) will allow for an open market place for the development of M2M applications. These applications can be integrated into the M2M network components and thus can extend the capabilities in a very flexible manner. These applications can be independent of the deployed communication technology and thus can address a much broader market place than specific applications.

Service provider can initially focus on specific domains using a standardised service layer and still having the possibility to extend the business towards new field if needed.

7.3 OGC Sensor Web for IoT

7.3.1 Location and Sensors in IoT

All IoT things are at a location. Location is a fundamental piece of information for most of the new and innovative applications enabled by IoT. Location information is ubiquitous but not always correct. Location data quality can be easy to maintain, but subtle mistakes can creep in and cause failures, damage and death. Accurate handling of location information in IoT is being built on the standards for location well established by several standards developing organizations, in particular as established by the Open Geospatial Consortium (OGC).[1]

Sensors and actuators associated with IoT devices are bringing a new awareness and control of the environments in which we live and work. To achieve this capability most broadly, observations made by sensors must

[1] The Open Geospatial Consortium: http://www.opengeospatial.org/

become as interoperable as the information accessible on the Web. Most sensor observations will not be used directly by humans but rather will be processed by software as the information goes from the sensor to the human. Here again IoT benefits from established standards.

The Open Geospatial Consortium (OGC) is an international industry consortium of 481 companies, government agencies and universities participating in a consensus process to develop publicly available interface standards. OGC® Standards support interoperable solutions that "geo-enable" the Web, location-based services and IoT.

7.3.2 OGC Sensor Web Enablement

"In much the same way that HTML and HTTP enabled WWW, OGC Sensor Web Enablement (SWE) will allow sensor webs to become a reality." This vision in 2001 by Dr. Mike Botts was a basis for initiating development of SWE. Due to the large number of sensor manufacturers and differing accompanying protocols, integrating diverse sensors into observation systems is not straightforward. A coherent infrastructure is needed to treat sensors in an interoperable, platform-independent and uniform way. SWE[2] standardizes web service interfaces and data encodings as building blocks for a Sensor Web (Figure 7.4). SWE standards are now mature specifications with approved OGC compliance test suites and tens of independent implementations. The SWE standards are deployed in operational systems, including safety critical systems.

The OGC SWE framework includes:

- **Sensor Observation Service (SOS)** — standard web interface for accessing observations and subscribing to alerts.
- **Sensor Planning Service (SPS)** — standard web interface for tasking sensor system, models, and actuators.
- **Web Notification Service (WNS)** — service for asynchronous dialogues (message interchanges) with one or more other services.
- **Sensor Alert Service (SAS)** — web service for publishing and subscribing alerts from sensor or simulation systems.

[2]OGC Sensor Web Enablement: http://www.ogcnetwork.net/swe

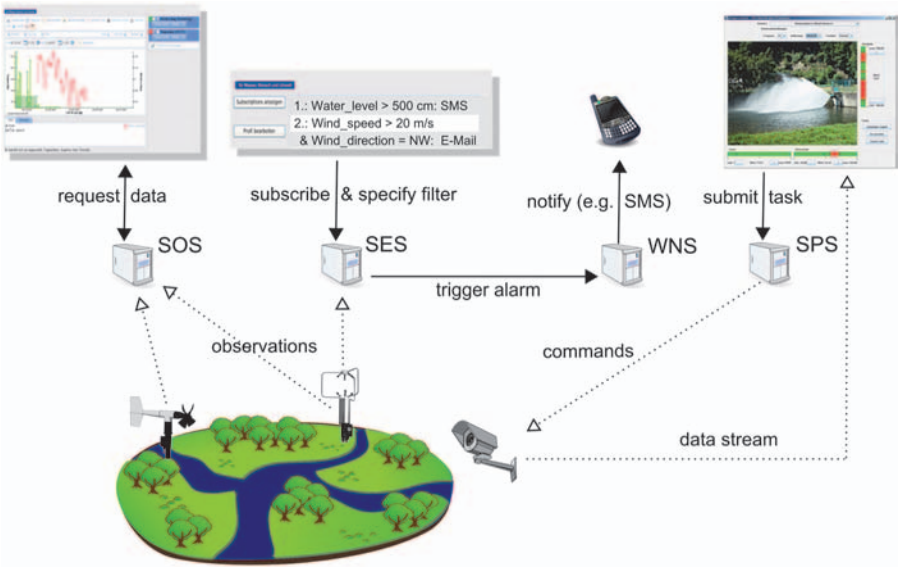

Fig. 7.4 Deployment scenario for OGC sensor web enablement. (*Source*: Bröring).[3]

- **SensorML** — models and schema for describing sensor and actuator systems and processes surrounding measurement and the tasking of assets.
- **Observations and Measurements (O&M)** — models and schema for packaging observations.

7.3.3 OGC SensorWeb for IoT Standards Working Group

Interoperability of IoT devices based on open standards will be required to meet the vision of IoT. Based on a series of community workshops, OGC members chartered development of a *Sensor Web for IoT* standard. OGC's existing standards for location information and sensor observations are the basis for this work. The new OGC Sensor Web for IoT Standards Working Group (SWG)[4] is to develop one or more standards based on existing protocols while leveraging the existing and proven OGC SWE family of standards.

[3] Bröring, A., *et al.* (2011): New Generation Sensor Web Enablement. Sensors, 11(3), pp. 2652–2699.
[4] OGC Sensor Web for IoT SWG: http://www.opengeospatial.org/projects/groups/sweiotswg

IoT has the potential to change the world, just as the Internet and WWW did. A huge variety of day-to-day objects will become IoT enabled. A plethora of applications, from personal interest to environmental monitoring, will emerge by mix-and-match of different sensors, mobile devices, and cloud-based resources. Heterogeneity of devices and applications (Figure 7.5) demands *interoperability*. The Sensor Web for IoT SWG aims for interoperability based on open standards as key factor for the success of IoT, resulting in a greater accessibility and utilization of IoT information (Figure 7.6).

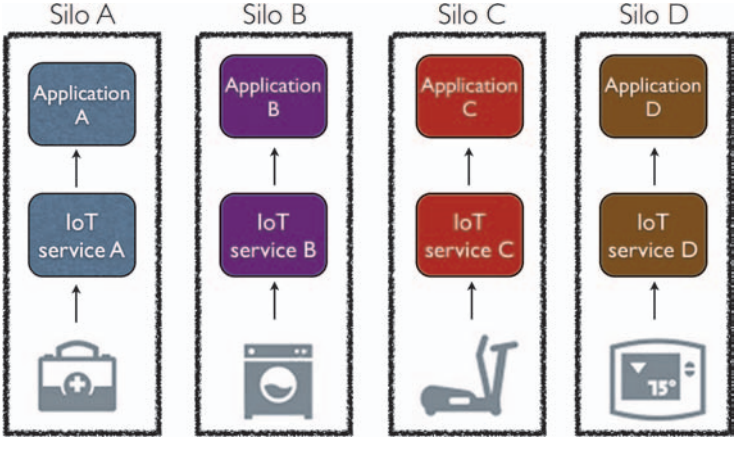

Fig. 7.5 Non-interoperable IoT sensing applications.

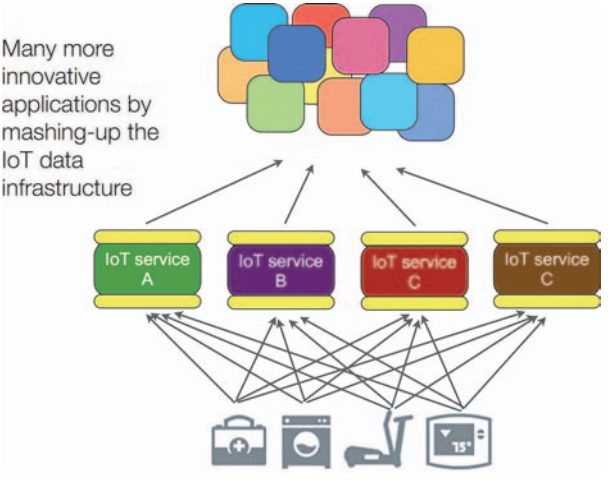
Many more innovative applications by mashing-up the IoT data infrastructure
IoT service A
IoT service B
IoT service C
IoT service C

Fig. 7.6 OGC sensor web for IoT interoperability.

Building on SWE and other IoT protocols, the *OGC Sensor Web for IoT SWG* is developing a standard that makes observations captured by IoT devices easily accessible. This functionality is defined as lightweight RESTful web interface using CRUD (i.e., create, read, update, and delete) functions on IoT resources. While nearly complete, Sensor Web for IoT is ongoing and OGC invites others to join the process to define an easy-to-use interface for sensors to realize the Open IoT vision.

ETSI and OGC are collaborating on LBS (Location-Based Services), Intelligent Transport Systems (ITS) and GNSS (Global Navigation Satellite Systems) in SUNRISE research project (www.sunrise-project.eu) funded by the European GNSS Agency (www.gsa.europe.eu) in the framework of 2 **Open GNSS Service Interface Forum** (sunrise.opengnssforum.eu). ETSI see here an opportunity for GNSS, Augmented Reality and IoT to collaborate on LBS.

7.4 IEEE and IETF

The main focus of the IEEE standardisation activities are on the lower protocol layers namely the Physical layer and the MAC layer. The IETF activities are positioned in the Networking and transport layer with some elements in the layers above, see Figure 7.2.

The IEEE laid an early foundation for the IoT with the IEEE802.15.4 standard for short range low power radios, typically operating in the industrial, scientific and medical (ISM) band. Having shown some limitations with the initial solutions such as Zigbee, the basic 15.4 MAC and PHY operations were enhanced in 2012 to accommodate the requirements of industrial automation and smartgrid metering. The new version of the standard introduced the 802.15.4g PHY, which allows for larger packets up to two Kilo-Octets and in particular comfortably fits the IPv6 minimum value for the maximum transmission unit (MTU) of 1280 octets, and the 802.15.4e MAC, which brings deterministic properties with the Time Slotted Channel Hopping (TSCH) mode of operation.

The value of the TSCH operation was initially demonstrated with the semi-proprietary wireless HART standard, which was further enhanced at the ISA as the ISA100.11a standard, sadly in an incompatible fashion. The most recognizable enhancement by ISA100.11a is probably the support of

IPv6, which came with the 6LoWPAN Header Compression, as defined by the IETF. Another competing protocol, WIAPA, was developed in parallel in China, adding to fragmentation of the industrial wireless automation market, and ultimately impeding its promised rapid growth.

A strong request is now coming from the early adopters, in the industrial Process Control space, for a single protocol that will unify those existing protocols in a backward compatible fashion, and extend them for distributed routing operations. Distributed operations are expected to lower the deployment costs and scale to thousands of nodes per wireless mesh network, enabling new applications in large scale monitoring. the 6TSCH Working Group is being formed at the IETF to address the networking piece of that unifying standard.

Based on open standards, 6TSCH will provide a complete suite of layer 3 and 4 protocols for distributed and centralized routing operation as well as deterministic packet switching over the IEEE802.15.4e TSCH MAC. Most of the required 6TSCH components already exist at the IETF in one form or another and mostly require adaptation to the particular case, and 6TSCH will mostly produce an architecture that binds those components together, and provide the missing glue and blocks either as in-house RFCs, or by pushing the work to the relevant Working Groups at the IETF.

Yet, there is at least one entirely new component required. That component, 6TUS, sits below the 6LoWPAN HC layer in order to place the frames on the appropriate time slots that the MAC supports, and switch frames that are propagated along tracks that represent a predetermined sequence of time slots along a path.

Centralized routing is probably a case where work will be pushed outside of the 6TSCH WG. That component will probably leverage work that was done at the Path Computation Element (PCE) Working Group, and require additions and changes such as operation over the CoAP protocol, and new methods for advertising links and metrics to the PCE. All this work probably belongs to the PCE WG. Another example is the adaptation of the IPv6 Neighbor Discovery (ND) protocol for wireless devices (WiND) that will extend the 6LoWPAN ND operation and will probably be conducted at the 6MAN working group in charge of IPv6 maintenance.

Distributed route computation and associated track reservation, on the other hand, can probably be addressed within the 6TSCH Working Group,

as it is expected to trivially extend the existing RSVP and RPL protocols. Same goes for PANA that may be extended to scale the authentication to the thousands of devices.

The next step for this work is a so called BoF in July 2013 in Berlin. The BoF will decide whether a WG should be formed and determine the charter for that WG.

IEEE ComSoc has appointed the key partners of the IOT6 project to lead the newly created IOT track within the Emerging Technologies Committee. IOT6 created a web site and attracted 400 members in the first 3 months: http://www.ipv6forum.com/iot//. IOT6 will use this platform to disseminate IOT6 solutions on a large scale basis. The Globecom IOT track is under preparation. http://www.ieee-globecom.org/CFP-GC13-SAC-IOT_final.pdf

7.5 ITU-T

The Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) is progressing standardization activities on Internet of Things (IoT) since 2005.

After a report on "The Internet of Things", published by the ITU in 2005, the ITU-T established a Joint Coordination Activity (JCA-NID), which aimed at sharing information and performing coordination in the field of network aspects of Identification systems, including RFID. The JCA-NID supported the work of the ITU-T Study Groups which led to the approval of initial Recommendations in the areas of tag-based identification services, Ubiquitous Sensor Networks (USN) and Ubiquitous Networking, and their application in Next Generation Networks (NGN) environment.

With the official recognition in 2011 of the centrality of IoT in the evolution of future network and service infrastructures, the JCA-NID was renamed as JCA-IoT (Joint Coordination Activity on Internet of Things) — itu.int/en/ITU-T/jca/iot — and the working structure of the IoT-GSI (IoT Global Standards Initiative) — http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx — was formally established. Since then, the ITU-T activities related to IoT have greatly expanded and produced additional Recommendations spanning various areas of application (e.g. networked vehicles, home networks, mobile payments, machine oriented communications, sensor control networks, gateway applications), as well as IoT framework aspects (basic concepts and

terminology, common requirements and capabilities, ecosystem and business models etc.) and, more recently, testing aspects.

Beyond the above mentioned IoT focused activities and the potential future IoT studies, which are included in the "IoT workplan" (a living list maintained by the IoT-GSI), it has to be noted that there are other ITU-T ongoing studies closely related to the IoT — it is worthwhile to mention here those related to Future Networks, Service Delivery Platforms and Cloud Computing.

In parallel with the JCA-IoT's coordination efforts with external entities and its maintenance of a cross-SDO list of IoT standard specifications and associated roadmap (the "IoT Standards Roadmap", freely available from the JCA-IoT web page), a remarkable milestone has been achieved by the IoT-GSI via the finalization in June 2012 of the ITU-T Recommendation Y.2060 "Overview of Internet of Things" [6]: the "IoT" is there defined — in fundamental alignment with the European IERC vision of IoT — as *"a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies"*. To note that, in this perspective, the Machine to Machine (M2M) communication capabilities are seen as an essential enabler of the IoT, but represent only a subset of the whole set of capabilities of IoT.

Among the various ITU-T IoT-related efforts, the Focus Group on M2M Service Layer (FG M2M) — http://www.itu.int/en/ITUT/focusgroups/m2m/Pages/default.aspx — deserves a special mention: established in 2012 with the key goal to study requirements and specifications for a common M2M Service Layer, it focuses its developments on the "e-health" application domain (priority scenarios being those of remote patient monitoring and assisted living). The FG M2M is also targeting the inclusion of vertical market stakeholders not part of the traditional ITU-T membership, such as the World Health Organization (WHO), and the collaboration with M2M and e-health communities and SDOs.

The FG M2M work is currently developing deliverables dealing with e-health use cases and ecosystem, M2M service layer requirements and architectural framework, APIs/protocols and e-health standardization gap analysis. In this context, the M2M service layer capabilities (Figure 7.8) aim to include those common to the support of different application domains as well as those required for the support of specific application domains.

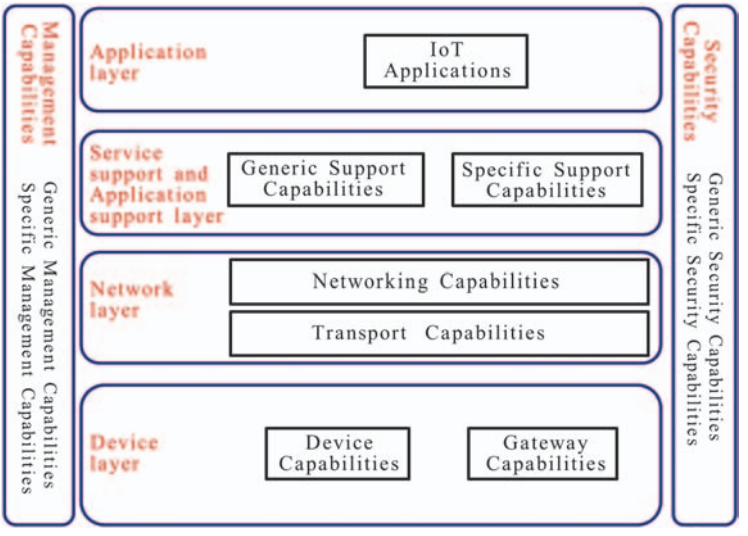

Fig. 7.7 IoT reference model.

(*Source*: ITU-T Y.2060).

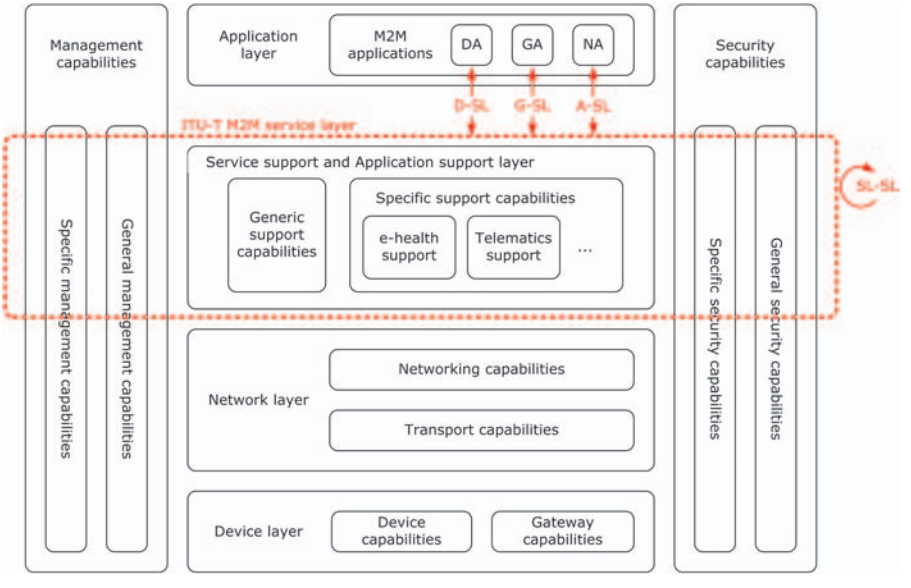

Fig. 7.8 The ITU-T M2M Service layer [work in progress in the FG M2M].

As highlighted by Marco Carugi (ITU-T Question 2/13 Rapporteur and vice-Chair of the FG M2M), representing ITU-T at the latest IERC/IoT standardisation coordination meeting in Delft (February 7–8 2013), IERC and ITU-T have entertained good relationships all along the IoT standardization activities of ITU-T, particularly in the context of JCA-IoT and IoT-GSI.

IERC has liaised with ITU-T and taken an active role in the discussions which led to the finalization of the ITU-T definition of "Internet of Things" and the approval of ITU-T Y.2060 (aspects related to IoT Reference Model (Figure 7.7), IoT Ecosystem, high-level requirements of IoT and other IoT definitions).

More recently, exchanges have taken place with respect to the IoT-A project in the context of requirements, capabilities and functional architecture of IoT (Question 2/13, FG M2M).

The ITU and IERC collaboration and coordination are expected to continue in the future and might involve also IoT "vertical" matters, for example e-health (FG M2M, ITU-T SG13 and SG16), Smart Cities (FG on Smart Cities), Smart Grids (JCA-SG&HN), Intelligent Transport Systems (FG CarCOM, collaboration initiative on ITS communication standards etc.).

7.6 Conclusions

There is a good momentum on M2M service layer standardisation, semantic interoperability and Future Networks standardisation as a main driver of the future success of integrated IoT. In this context, the OGC activities bring important inputs to the oneM2M and ETSI M2M activities. In addition several PHY and MAC layer standards activities in IEEE, ETSI (low power DECT) and other groups will provide required lower layer enabling technologies for the integration into the overall IoT.

IERC and its participating projects are seen as a catalyst and an European IoT coordination platform facilitating international world-wide dialog. IoT Workshops co-organised between the European Commission, IoT Research and innovation projects, IoT Industry Stakeholders and IoT Standard Organisation groups should continue. These workshops should facilitate Interoperability Testing events to stimulate IoT community building to reach consensus

on IoT standards common developments on all protocol layers. The results of these events can be seen as an essential input for the further development and evolution of the IoT standardisation. New domains have to be integrated into the overall view like the standardisation development in ITS (Intelligent Transport Systems) in ETSI and ISO.

A significant effort will be required to come to an overall cross vertical IoT vision and interoperable standards environments.

References

[1] ETSI Technical Specification TS 102 689: “M2M Service requirements", Sophia Antipolis, France, 2012.
[2] ETSI Technical Specification TS 102 690: “M2M Functional Architecture", Sophia Antipolis, France, 2012.
[3] ETSI Technical Specification TS 102 921: “M2M mla, dla and mld interfaces", Sophia Antipolis, France, 2012.
[4] ETSI Technical Report TR 102 966: “Interworking with M2M area Networks". Sophia Antipolis, France, 2012.
[5] ETSI Technical Report TR 101 531: “Reuse of Core Network Functionalities by M2M Service Capabilities”, Sophia Antipolis, France, 2012.
[6] ITU-T Recommendation Y.2060: “Overview of the Internet of Things”, Geneva, Switzerland, 2012.

8

Simpler IoT Word(s) of Tomorrow, More Interoperability Challenges to Cope Today

Payam Barnaghi[1], Philippe Cousin[2], Pedro Maló[3], Martin Serrano[4], and Cesar Viho[5]

[1]*University of Surrey, United Kingdom.*
[2]*Easy Global Market, France.*
[3]*FCT-UNL/UNINOVA-CTS, Portugal.*
[4]*DERI NUI-Galway, Digital Enterprise Research Institute, Ireland.*
[5]*University of Rennes I, France.*

8.1 Introduction

In this chapter we review recent trends and challenges on interoperability, discuss physical versus virtual and while addressing technology interoperability challenges in parallel, discuss how, with the growing importance of data understanding and processing, semantic web and their technologies, frameworks and information models can support data interoperability in the design of the Future Internet. Internet of Things (IoT) is taken as reference example in enterprise applications and services and their importance of the economic dimension.

Extensible discussed the Internet of Things (IoT) refers to things ("objects") and the virtual representations of these objects on the Internet. IoT defines how the things will be connected through the Internet and how those things "talk" amongst other things and communicate with other systems in order to expose their capabilities and functionalities "services". Internet of

Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, 277–314.
© 2013 *River Publishers. All rights reserved.*

Things is not only linking connected electronic devices by using the Internet; it is also web-enabled data exchange in order to enable systems with more capacities "smartness". In other words IoT aims for integrating the physical world with the virtual world by using the Internet as the medium to communicate and exchange information.

Technically speaking IoT is mainly supported by continuous progress in wireless sensor networks software applications and by manufacturing low cost and energy efficient hardware for sensor and device communications. However, heterogeneity of underlying devices and communication technologies and interoperability in different layers, from communication and seamless integration of devices to interoperability of data generated by the IoT resources, is a challenge for expanding generic IoT solutions to a global scale.

In this article we present various parallel and inter-related interoperability challenges ensuring that technologies deliver information in a seamless manner while this information is understood whatever the context and efficiently processed to deliver the potential of innovative services we are looking for.

To make everything simpler in our life tomorrow in using any object, any information, anywhere we need to solve complex interoperability issues today.

8.1.1 Different Types of Interoperability

First we need to understand interoperability. The main objective of this article is not to produce a new definition on interoperability but explore the different roles and functionality interoperability plays in the Internet of Things today. In this sense there are many definitions of interoperability but for instance in the context of the 3rd Generation Partnership Project, 3GPP, interoperability is:

> "*the ability of two or more systems or components to exchange data and use information*"

This definition is interesting as provide many challenges on how to:

- Get the information,
- Exchange data, and
- Use the information in understanding it and being able to process it.

A simple representation of interoperability can be seen as follow:

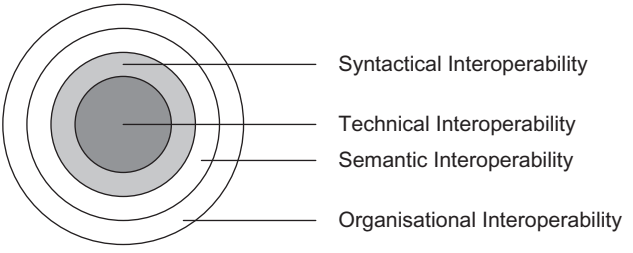

Fig. 8.1 The Dimensions of Interoperability.

In a white paper on interoperability [29], we can get the following definition(s):

> **Technical Interoperability** is usually associated with hardware/ software components, systems and platforms that enable machine-to-machine communication to take place. This kind of interoperability is often centred on (communication) protocols and the infrastructure needed for those protocols to operate.
> **Syntactical Interoperability** is usually associated with data formats. Certainly, the messages transferred by communication protocols need to have a well-defined syntax and encoding, even if it is only in the form of bit-tables. However, many protocols carry data or content, and this can be represented using high-level transfer syntaxes such as HTML, XML or ASN.1
> **Semantic Interoperability** is usually associated with the meaning of content and concerns the human rather than machine *interpretation* of the content. Thus, interoperability on this level means that there is a common understanding between people of the meaning of the content (information) being exchanged.
> **Organizational Interoperability**, as the name implies, is the ability of organizations to effectively communicate and transfer (meaningful) data (information) even though they may be using a variety of different information systems over widely different infrastructures, possibly across different geographic regions and cultures. Organizational interoperability depends on successful technical, syntactical and semantic interoperability.

> We can add two other dimensions: **Static and dynamic interoperability**

We should not also forget that two products couldn't interoperate if they don't implement the same set of options. Therefore when specifications are including a broad range of options, this aspect could lead to serious interoperability problem. Solutions to overcome these aspects consist of definition clearly in a clear document the full list options with all conditions (e.g. defined as PICS in [38]) as well as to define set of profiles. In the later case, defining profile would help to truly check interoperability between two products in the same family or from different family if the feature checked belong to the two groups. We could consider this aspect as **static interoperability** using approach of the well-known OSI overall test methodology ISO 9646 [38], where there is definition of static conformance review. Conformance testing consists of checking whether an IUT (Implementation Under Test) satisfies all *static and dynamic* conformance requirements. For the static conformance requirements this means a rev-iewing process of the options (PICS) delivered with the IUT. This is referred to as the static conformance review.

This aspect could appear easy but that represent serious challenge in the IoT field due the broad range of applications.

In the meantime, in front of growing complexity we also noticed many solutions to adapt to non-interoperability leading to be able to communicate and understand. One interesting research as presented by "eternal interoperability" here in one of the section below consists to accept differences and potential non-interoperability for instance between two different protocols but to adapt on the fly. We see also such features in intelligent gateways and middlewares. This can be called **dynamic interoperability** and should be a continuous important research area in particular with the growing complexity and heterogeneity of IoT environments.

8.1.2 The challenges

The overall challenges in interoperability is first to stabilize the foundation of the real world, ensuring technical interoperability from technologies to deliver mass of information and then complementary challenges are for the information to be understood and processed. Before entering into details we

will in the tables below present a summary of the challenges for technical and semantic interoperability.

IoT Technical Interoperability Challenges/Requirements

Requirement(s)	Rationale & Remarks
Best practices awareness • Avoid spreading effort in addressing interoperability for worldwide protocols	• Coordinate worldwide interoperability initiatives on market support specifications or protocols • Develop market acceptance roadmap • Use clear specifications development and testing methodologies leading to improve quality while reducing time and costs in a full chain optimized development cycle • Define if needed profiles to improve interoperability
Validation of specifications • Reduce ambiguities in specifications and development time	• Specifications development time could be too long • Ambiguities in specifications could lead to major non interoperability issues • Quality, time and cost factors lead to the needs of models and automation
Tests specifications • Provide market accepted test specifications ensuring minimum accepted level of interoperability	• No test specifications lead inevitably to different specifications implementation and interoperability issues • Development test specifications is often too expensive for limited set of stake holders and effort should be collectively shared • Tools processing and automation are only way to reduce time and market (e.g. use of MBT)
Tools and validation programmes • Develop market accepted and affordable test tools used in market accepted validation programmes	• Development of test tools are expensive • Available test tools developed spontaneously by market forces can have test scopes overlapping and even not answering to all tests needs. • Full chain of specifications to tool development not considered • Providing final confidence to end users with consistent tests not always considered

The following table/ lists summarize the main requirements associated with the development of the IoT service(s)/application(s) in reference to

semantic interoperability requirements and moreover, it provides the main rationale that has led to these requirements.

IoT Semantic Interoperability Challenges/Requirements

Requirement(s)	Rationale & Remarks
Integration • Support multiple ICOs (sensors, actuators) and relevant types of data sources (independently of vendor and ICO location).	• Enable scalable sharing and integration of distributed data sources. • All IoT applications involve multiple heterogeneous devices. • Orchestrate ICOs in order to automatically formulate composite workflows as required by end-user applications.
Annotation • Enable the (automated) linking of relevant data sources.	• Linking of data sources facilitates application integration and reuse of data. • Enable interactions between ICOs and between IoT services. • Built on the standards (i.e. W3C SSN standard ontology) for description of sensors and ICOs.
Management • Enable the creation and management of virtual sensors and virtual ICOs based on the composition and fusion of streams stemming from multiple (ICO) data sources.	• Application development and integration involves multiple distributed and heterogeneous data sources to be processed in parallel. • The definition and management of virtual sensors eases applications integration.
Discovery • Provide the means for discovering and selecting ICOs and data sources pertaining to application requests (according to their capabilities).	• End users need a high-level interface to be accessed. • Provide the means for describing/formulating IoT services and applications according to high-level descriptions. • Provide (configurable) visualisation capabilities of multiple integrated data sources (in a mashup fashion).
Analysis and Reasoning • Provide analytical and reasoning tools on top of semantic level capabilities.	• IoT addresses large-scale environments with numerous ICOs featuring different functionalities and capabilities. • End-user applications involve the monitoring of virtual and/or Physical sensors

(*Continued*)

(*Continued*)

Requirement(s)	Rationale & Remarks
Visualisation • Optimise usage of resources (storage, computing cycle, sensor utilisation) across multiple users sharing these resources.	• Several applications involve object-to-object (e.g., M2M) interactions or interactions between services; such interactions could be either defined explicitly (i.e. by end users) or derive implicitly (based on the application context).

8.2 Physical vs Virtual

Towards enabling a new range of large-scale intelligent Internet connected objects (ICO) services and applications the Internet of Things (IoT) applications and the cloud computing delivery models play a crucial role. In other words the IoT area therefore serves as a blueprint for non-trivial ICO scalable applications, which will be delivered in an autonomic fashion and according to cloud-based utility models. It has been extensively discussed Internet of things (IoT), sometimes indistinctly named Internet-connected objects (ICO's) will be an integral component of the Future Internet. Indeed, the proliferation of applications involving Internet-connected objects, has recently given rise to the notion of networks of internet-connected objects, which are promoted as large-scale networks of spatially distributed physical devices or entities called "sensors" with scalable processing and storage capabilities. However, there is still no easy way to formulate and manage networked environments of internet-connected objects i.e. environments comprising "sensors" and offering relevant utility-based (i.e. pay-as-you-go) services.

IoT environments for Internet-connected objects will greatly facilitate the deployment and delivery of applications, since they will enable businesses and citizens to select appropriate data and service providers rather than having to deploy physical devices commonly called sensors. At the same time, they will provide capabilities (such as on-demand large scale sensing), beyond what is nowadays possible.

It is important to highlight the origins of IoT are found in the area of (Radio Frequency IDentification) RFID domain where RFID tags are extensively used for data collection. The static information a group of RFID tags can generate motivated the quick development of RFID middleware frameworks to the extent that nowadays FID frameworks provides functionality for RFID data

collection, filtering, event generation, as well as translation of tag streams into business semantics.

Several initiatives have produced several open-source RFID frameworks, such as Mobitec [41], Aspire RFID [42] as well as the fosstrak project [43] which provide royalty-free implementations of RFID middleware stacks. The evolution has continued and the generators of data are now generally named "sensors" by their capacity to produce data and their flexibility to create cells or groups of them by using embedded wireless technology. In this sense several middleware platforms have also been devised in the area of WSN (Wireless Sensor Networks). Specifically, there are platforms addressing only the level of the sensor network, whereas other deal also with devices and networks connected to the WSN. Some middleware platforms are characterized as sensor databases, other as virtual machines, whereas there are also publish-subscribe approaches. Systems such as Moteview [44] and ScatterViewer [45] are examples of WSN development and monitoring systems, which however provide limited extensibility (tightly coupled approach).

Other environments such as Hourglass [46], SenseWeb [47], jWebDust [48] and GSN [49] provide more complete development and/or programming environments for WSN applications.

Beyond the limits of physical devices known as "sensors" exist the notion of "Virtual Sensor" virtual sensors from the basis concept is a core representation of an element of the IoT platforms representing new data sources created from live data. These virtual sensors can filter, aggregate or transform the data. From an end-user perspective, both virtual and physical sensors are very closely related concepts since they both, simply speaking, measured data. The Semantic Sensor Network (SSN) ontology, providing the most important core vocabulary for sensing data, defines the notion of sensor and physical devices in general, therefore formally the concept of a virtual sensor as a subclass of the sensor concept as defined in the SSN ontology. Due to the rising popularity of IoT technologies and applications the emergence of a wide range of platforms that enable users to build and/or use IoT applications is unavoidable. In general there is a clear trend towards the convergence of physical worlds and virtual solutions by using IoT technologies.

In all cases either Physical or Virtual sensors, a middleware framework is the core element to be used for providing baseline sensor functionalities associated with registering and looking up internet-connected objects,

exchanging messages between objects, as well as fusing and reasoning data from multiple-objects.

Some other features in the order of these implementations are:

- integrate ontologies and semantic structures, in order to enable semantic interactions and interoperability between the various objects, which will be a significant advancement over the existing syntactic interactions.
- provide Open Linked Data interfaces (e.g., SPARQL (SPARQL Protocol and RDF Query Language) over ontologies for internet-connected objects within the physical world middleware to interact with virtual world).
- Define techniques for the automated data configuration of filtering, fusion and reasoning mechanisms, according to the problems/tasks at hand.

8.3 Solve the Basic First — The Physical Word

The future Internet architecture will consist of a core network and its components and an access network based on wired and wireless systems. These wireless networks represent a future of billions of information devices embedded in the physical world will run a standard internetworking protocol that ensures interoperability between different kinds of networks.

Ensuring technical interoperability

Experience in observing deployment of successful interoperable products for many technologies [35, 36, 37] lead to the identification of some activities, which are impacting the technical interoperability

1. Quality of the base specifications
2. Availability and quality of consistent test specifications
3. Availability of good and affordable test tools
4. Organization of the validation environment

Specifications: All technology development starts from a stable specification. This is only one part of the design phase of an eventual product, but it is a critical part. A poor specification will inevitably lead to interoperability

problems in real systems. A specific attention should be paid then to improve the quality of specifications using several approaches which can be using clear development guidelines, formal notation (i.e. SDL, UML) when feasible and organize validation exercise which can include interoperability events or named plugfests or plugtest [35].

Tests specifications: Once specifications are stable and eventually "validated", the second step is to provide to the development community some tests specification. This step is often a challenge, as some believe this part should be left to the market forces for proving that developments follow the specifications. Some ideas also are promoted that going to interoperability events can demonstrate that but more than 10 years of experience in organizing interoperability events [35] makes evidence that interoperability events useful tools but cannot replace the need of some market accepted tests specifications. Debates exist on the depth of such specifications, as such activity is resources consuming. We will discuss later on the important economic factor but this issue can be solved in resource optimization and in using modern approach with well-recognized notation (e.g. TTCN3) and eventually MBT (model Based testing) approach allowing a lot of possible automation. In any case interoperability cannot be guarantee without a minimum of available and also validated test specifications. This important statement is still not today really supported by many technical communities and this represents in itself a challenge.

Test tools: tests need to be executed in test environment and this aspect does not require at the beginning high attention in particular by technology decision-maker. However no product can interoperate if we cannot check and prove some features are conformed to the specifications. Developing tools is again highly expensive and some communities prefer to let this complex matter to the market forces pretending not be able to finance collectively test tools and even not seen the reason why doing so. Experience [35] demonstrates the approach of no cost, no expenses in testing matter could lead to more expenses for the community at the end in front of a lot of non-interoperable issues that such approach will finally generated. Solid validation or certification programs such in Bluetooth, GSM, 3G, Wifi , Zigbee,, just to mention few , recognize the importance of having well defined test tools. Here once gain, more than 20 years of experience in interoperability [29] make evidence that there are

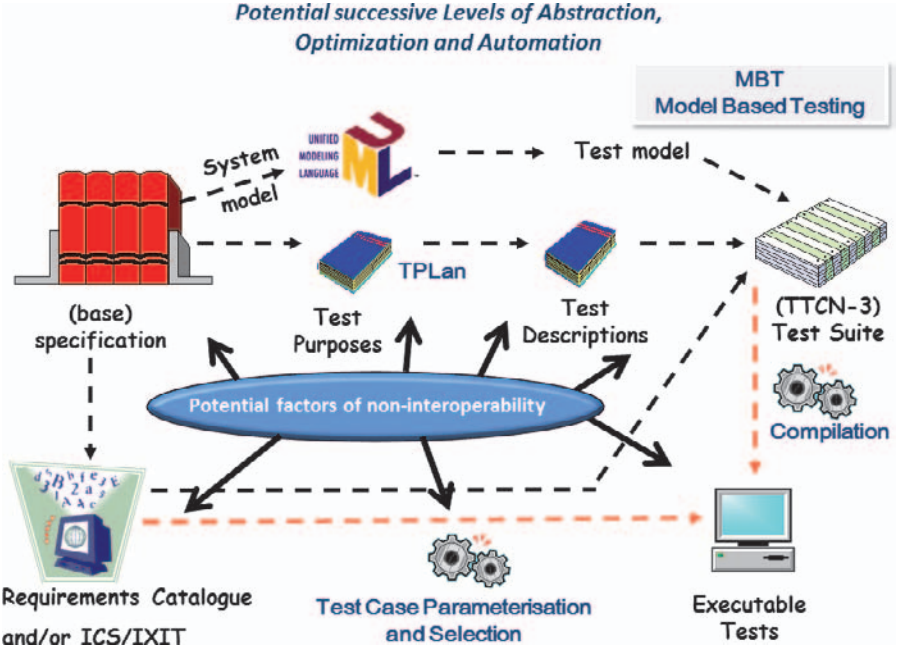

Fig. 8.2 Full development chain with interoperability factors.

many factors which would lead to non-interoperability and which should be tackle one by one in the overall interoperability development chain.

Cases of 6lowpan and CoAP

The figure below represents a simplified overview of layers and protocols which are currently considered for an IoT. The Probe-It project look at protocol such as 6lowpan and CoAP to get some status on what are the current practices to ensure interoperability and how such practices are overcome non-interoperability potential factors as presented in the previous section. Situation was found that such important and market supported protocols are still at the earlier stage of developing test specifications and tools and the current situation cannot ensure the level of interoperability the world wide market is looking for and for such a mass market ambition.

6lowPAN is an acronym of IPv6 over LoW Power wireless Area Networks. 6lowpan is also the name of a working group in the Internet area of the

IETF. The 6lowpan group has defined encapsulation and header compression mechanisms that allow IPv6 packets to be sent to and received from over IEEE 802.15.4 based networks. Beyond the usual differences between wireless access networks, mapping from the IPv6 network to the IEEE 802.15.4 based network poses additional design challenges with associated interoperability issues such as: Adapting the packet sizes of the two types of networks, Address resolution, Adaptation layer for interoperability and packet formats, Routing considerations and protocols, Device and service discovery, etc. These interoperability issues have to be considered at each level and need expertise both on IP protocol level as well as on IEEE 802.15.4 based networks together with a high knowledge in test development and methodology. The problem is that it is a huge task and initiatives to tackle these issues are not enough coordinated. Currently there are no market validated test specifications and tools. Plugfests such as the one to be organised end July 2013 [39] are good tool to help identifying the interoperability issues as well as to create a collective interest to progress interoperability

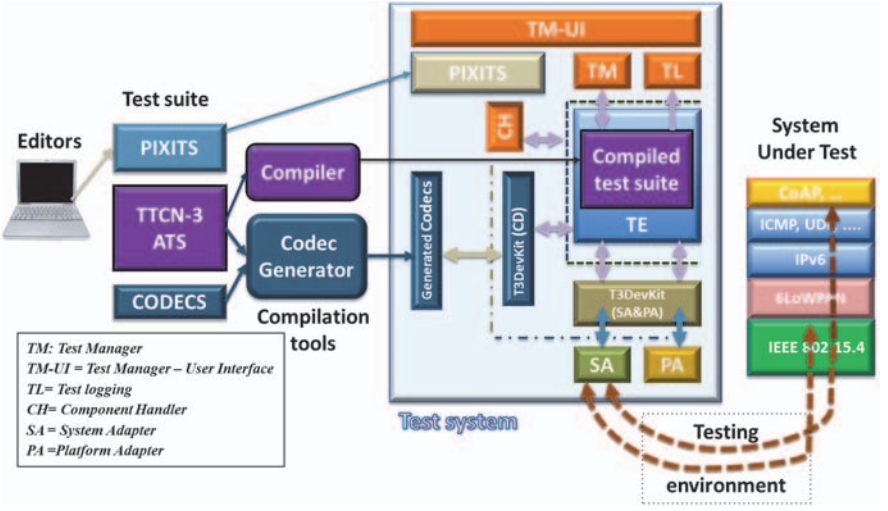

Fig. 8.4 Use of standardised methodologies for optimizing 6lowpan and CoAP protocols tests.

Constrained Application Protocol (CoAP) is a specialized web transfer protocol which is designed by CoRE working group of IETF keeping in mind the various issues of constrained environment to realize interoperations with constrained networks and nodes for machine to machine (M2M) applications like smart energy, building automation, smart home etc. CoAP could be one of the technologies identified for Internet of Things vision. Here again there are good progresses toward interoperability with interoperability events organised [40] but there is still a need for finalizing further test specifications and tools.

Probe-IT project develop some tests and tools on CoAP and 6lowPAN to demonstrate that it is possible to use market proof test methodologies which can be used for such protocols and can bring a lot of level of optimization and automation leading to improve quality while reducing time and costs.

Finally to guarantee a global (technical) interoperability of future interconnected objects, the previous examples described below show that there is an urgent need to coordinate all these initiatives with a roadmap including some common agreed method(s) that will help in answering at least the following questions:

- Are the existing testing methods suitable enough for these high combinatory complexities in IoT testing?

- How to manage the different levels of interoperability required? How to ensure testing coverage?
- What are the needs towards more suitable interoperability testing architecture, methodology and tools? What are the requested research activities to be achieved in the meantime?
- How can we improve the interaction of the different IoT testing initiatives?
- How can we optimize quality, time and costs in addressing interoperability?

8.4 The Data Interoperability

In the IoT framework, sensors and devices provide data about physical world objects. The observation and measurement of data related to an "*object*" or "*entity*" of interest can be related to an event or situation in the physical world. The process of turning this data into knowledge and perception and using it for decision-making, automated control, etc. is an important step task in IoT. The data can be provided by different stakeholders and from various sources. The quality of data can also vary depending on the sensing device, environmental variables and service/data providers. In addition to security and privacy issues related to IoT data, trust and reliability of the data and quality measures will be also important for real-world use case scenarios and business process integration in dealing with the IoT data. Seamless processing and interpretation of the IoT data requires common agreements on providing and describing the IoT data and also requires common service and interfaces descriptions to enable accessing to the IoT resource and devices. Considering the diversity of data types, device types and potential providers in the IoT domain, common service and data description frameworks are essential to describe and represent the services and the data to make it seamlessly accessible and process-able across different platforms and stakeholders.

The key goal of collecting and communicating data collected by various sensors and devices form the real world is to create situation awareness and enable human and machines to understand their surrounding environment better. This understanding of the situation enables creating smarter services and applications that can respond to the changes in their environment and can support machine processes or human user in intelligent decision making

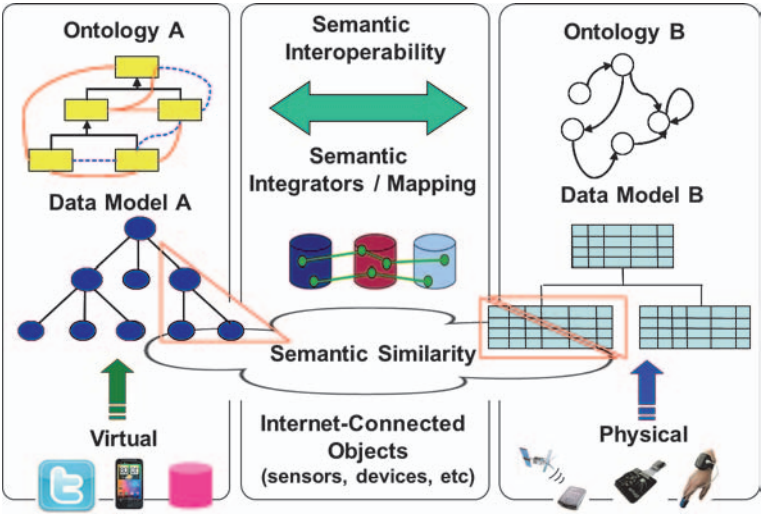

Fig. 8.5 Semantic interoperability for Internet-connected objects.

processes. However, the data collected by different sensors and devices from the real world is dynamic, the quality of data can vary over different devices and through the time, the data is location and time dependent and there are large number of resources than can create deluge of heterogeneous data. This makes processing, integrating and interpreting the real world data a challenging task.

While objects in IoT can be integrated into the service and application domain and devices can sense the environment, change the status of the objects, and respond to events, interpreting the data for managing the resources and their communication with each other and enabling seamless interaction between high-level services and devices are complex tasks that involve different technologies and solutions. Considering the fact that many of the devices and resources in IoT are heterogeneous, interoperability between different devices and their data is one of the key issues in this domain. The research in this area has recently gained momentum and is supported by new communication protocols, standards and methods that consider the dynamicity and heterogeneity of the underlying devices and resources and enable internetworking and interactions on IoT. However, the current IoT data communications often rely on binary or syntactic data models that are often unable to provide machine-interpretable meanings for the data. This hinders the creation of common tools and mechanisms to process and interpret the IoT data on a

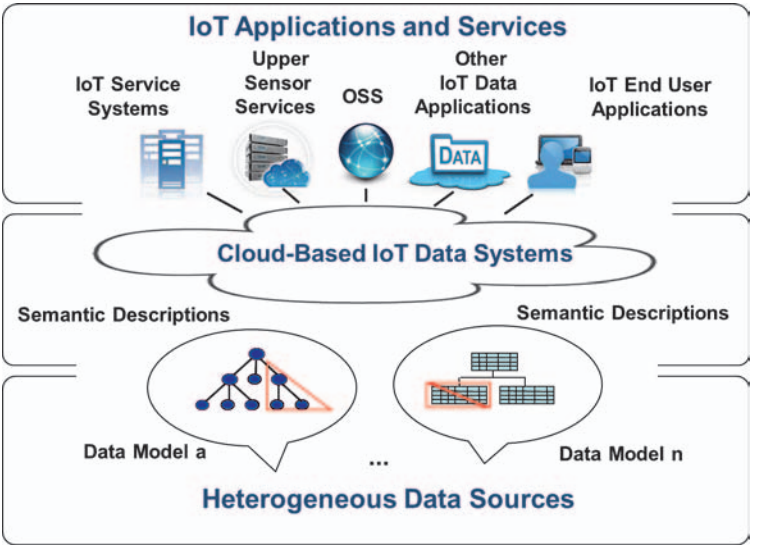

Fig. 8.6 The role of semantic interoperability for IoT applications and services.

large scale that can be supported by different stakeholders in a global framework. In general, large-scale platforms are required to support discovery and access to the resources, enable autonomous interactions with the resources, and use self-descriptive data and association mechanisms to process and interpret the IoT data, and integrate it into the high-level applications and service layers.

Semantic interoperability of the IoT data will ensure that data that is provided from different sources and by various providers is unambiguously accessible and process-able across different domains and stakeholders. The semantic annotation of the data can be created when an observation or measurement is created, or it can be added to the data when it is received via a gateway node. The semantic annotation, however, is not only annotation of the observation and measurement data. Effective discovery, access, management and utilisation of the IoT resource require machine-interpretable descriptions of different components and resources in the IoT framework (e.g. sensors, actuators, platform and network resources). The semantic interoperable description of services and interfaces that enable communication between different components in accessing, managing and using the IoT data and resources is also another important aspect that is supported by defining common models and standard representation frameworks. The IoT community now requires more

coordinated efforts to agree on common vocabularies and standards to describe data, resources and interfaces in the IoT domain. The representation frameworks should be also optimised to support more effective communication of the semantic annotated data across different resource constrained nodes.

8.5 The Semantic Interoperability

In recent years convergence between Internet technologies for communication's, computation's and storage's networks and the semantic web has been a clear trend in the Information and Communications Technology (ICT) domain [1]. Although widely discussed and researched, this trend has not fully run its course in terms of implementation, due to many complex issues involving deployment of non-interoperable and management infrastructural aspects, bottlenecks in the telecommunication systems, laciness on interoperability of big data processing in computing and Internet systems and also due to technological, social and economic restrictions in the ICT sector.

Telecommunications networks have undergone a radical shift from a traditional circuit-switched environment with heavy/complex signalling focused on applications-oriented perspective, towards a converged service-oriented space, mostly Internet-based systems interaction by customer as end-user and network operators as service providers with the semantic web as main enabler. In this radical shift services and networks follow a common goal: to provide solutions (services and applications) in a form of implemented interoperable data mechanisms [2]. The business benefits of this shift significantly reflect cost reduction and increase systems flexibility to react to user data demands, by replacing a plethora of proprietary hardware and ad-hoc software platforms with generic solutions supporting standardised development and deployment stacks.

In the other hand emergence and wide-scale deployment of wireless access network technologies calls into question the viability of basing the future Internet-based solutions on IP and TCP — protocols that were never intended for use across highly unreliable and volatile wireless interfaces. The GENI NSF-funded initiative to rebuild the Internet [3], argue that the future lies in layers of overlay networks that can meet various requirements whilst keeping a very simplistic, almost unmanaged, IP for the underlying Future Internet design. Others initiatives such as Clean Slate program, Stanford University

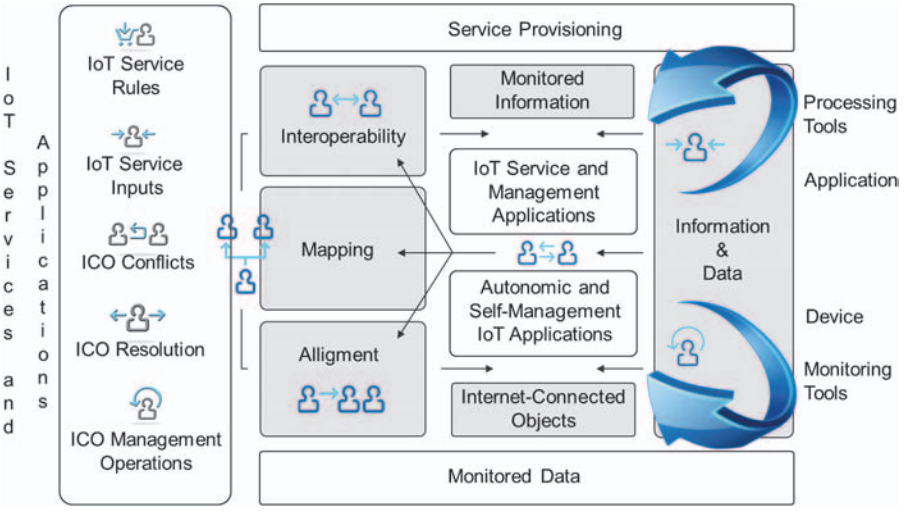

Fig. 8.7 Semantic interoperability control loop in IoT for services and applications.

[4], and Architecture Design Project for New Generation Network [5] argue that the importance of wireless access networks requires a more fundamental redesign of the core Internet Protocols themselves.

Likewise the pervasiveness of the physical devices and objects, resource constraints such as memory and power limitations on daily life devices, heterogeneity of the platforms and communication protocols create new challenges in inter-networking technologies and interaction mechanisms that enable interaction between data provides and consumers in the multiple domains. These challenges have raised new issues that are reflected in the recent architecture, design and development efforts for the Future Internet [6].

The interaction of the physical devices "objects" amongst other objects bring some implications on resource constraints such as memory and power limitations, likewise heterogeneity of the platforms and communication protocols create new challenges in inter-networking technologies and for data interaction mechanisms enabling interaction between data providers and consumers. Particularly in the IoT domain those interactions are generating a big challenge in order to establish common ways to interact and/or simply exchange information between the objects.

IoT has raised new issues that are reflected in the recent Internet architecture, important aspects to consider as design and development efforts for the

Future Internet [7]. The research in IoT has recently gained momentum and is supported by new communication protocols, standards and methods that consider the dynamicity and heterogeneity of the underlying devices and resources and enable internetworking and interactions on IoT. However, the current IoT data communications often rely on binary or syntactic data models that are unable to provide machine-interpretable representation of the data. This hinders the creation of common tools and mechanisms to process and interpret the IoT data on a large scale that can be supported by different stakeholders in a global framework. In general, large-scale platforms require to support discovery and access to the resources, enable autonomous interactions with the resources, and use self-descriptive data and association mechanisms to process and interpret the IoT data, and integrate it into the high-level applications and service layers. To achieve global IoT data distribution and utilisation, semantic interoperability between IoT resources and data providers and consumers is a key issue. This will also support effective discovery, query, interpretation and integration of the IoT data. Semantic interoperability ensures that data can be comprehended unambiguously by human users and software programs across different platforms [8].

Automated processing and interpretation of the IoT data requires common agreements on providing and describing the IoT data. To evaluate the quality aspects of data, the source provider, device and environment specific information also need to be associated to the data. Considering the diversity of data types, device types and potential providers in the IoT domain, common description frameworks are essential to describe and represent the data to make it seamlessly accessible and process-able across different platforms and stakeholders.

In general, to achieve automated and seamless integration of the IoT data in business applications and services, semantic description of different resources in the IoT domain is a key task. The aforementioned works are some examples of the recent efforts that have been made to address this issue. The semantic descriptions and annotations need to be provided at "Things" level (e.g. entity model described in [9], OGC O&M model), device and network level (e.g. W3C SSN ontology [10]), Service level (e.g. SemSoS [11]), and interaction and business process model (e.g. the IoT-aware business process modelling described in [12]) to enable autonomous processing and interpretation of the IoT data by different stakeholders in IoT business process lifecycle.

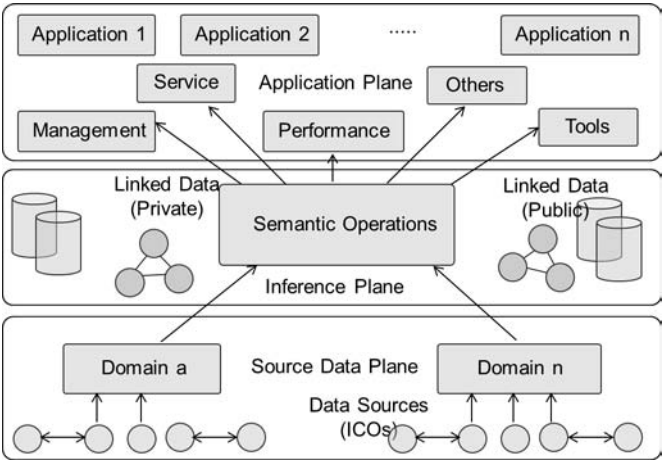

Fig. 8.8 Service Openness in IoT for Services and Applications.

In is important to note that just providing semantic annotations alone does not provide semantic interoperability on a global scale. The semantic description still needs to be shared, processed and interpreted by various applications and services across different domains and by different stakeholders.

Semantic interoperability of the IoT data will ensure that data that is provided from different sources and by various providers is unambiguously accessible and process-able across different domains and stakeholders. The semantic annotation of the data can be created when an observation or measurement is created, or it can be added to the data when it is received via a middleware gateway node. The semantic annotation, however, is not only annotation of the observation and measurement data. Effective discovery, access, management and utilisation of the IoT resource require machine-interpretable descriptions of different components and resources in the IoT framework (e.g. sensors, actuators, and network resources). The semantic interoperable description of services and interfaces that enable communication between different components in accessing, managing and using the IoT data and resources is also another important aspect that is supported by defining common models and standard representation frameworks. The current semantic Web technologies provide mechanisms to represent and process the semantic data. Information modelling and ontology creation efforts also define and describe different aspects of the IoT data and resources.

As IoT environments are often dynamic and pervasive, updating and managing the semantic descriptions is another key challenge for the resource providers. As discussed earlier, scalability of the solutions is a significant concern in designing solutions for IoT. This requires further efforts to define global standards, description models and representation frameworks that can describe the IoT data and services and provide optimised solutions which take into consideration the constraints and dynamicity of the IoT domain.

In many research and development communities the composition of data models for enabling information interoperability focuses on using semantic models (Ontology models) by means of annotated data to enable extensible, reusable, common and manageable linked-data plane. Previously referenced as inference plane [13], the linked-data plane uses semantic technologies for supporting interoperability and the required extensibility in handling end-user contents for pervasive applications.

The concept of the Linked Data originates from the need to interlinking individual data items and information objects to support semantic query and inferences on the data coming from the physical and virtual objects. The Linked Data, represented using formal knowledge representation formalisms, (i.e., the collection of semantic technologies such as RDF [13] and OWL [15, 16]), provides potential for information reuse and interoperability among heterogeneous sources. Different from the traditional ways of publishing information where datasets are simply made available on the Web, information published for the Linked Data is structured and connected to each other using logical constructs in widely used ontologies, such as FOAF [17] and SKOS [18], to form the Web of data.

The principles of publishing the Linked Data encourages reusing of existing information rather creating new one. Applications and human users can exploit the existing knowledge base by simply providing links to the data in it. DBpedia[1] is one of the most notable examples of the Linked Data, which extracts structured information from the Wikipedia. It enables not only sophisticated queries over the amazing amount of crowd-sourced information but also new ways of browsing and navigation through the semantic links.

The IoT manifests high degree of heterogeneity in many ways from the different types of things in the real world to different models for representing those

[1] http://dbpedia.org/

things. The resulting interoperability problem makes identifying, discovering and searching things on the global scale on the Internet a challenging task. In the past few years, researchers have proposed to use the semantic and service oriented technologies to address the interoperability issue. Many of the research efforts have been focussing on developing semantic models for annotating the things in the IoT domain. One of the most notable works in this line is the development of the W3C's Semantic Sensor Network (SSN) ontology [19]. The SSN ontology aims to model the sensors (and sensor networks), which are one category of the things. Later, the work in [20] has tried to provide a holistic modelling of the IoT domain concepts (e.g., entity of interests, physical and indoor locations, unit of measurement and so on); in particular, to hide the heterogeneity and complexity of the underlying devices (e.g., sensors), the modelling for services is proposed. The idea behind this is that a service exposes the functionalities that can be provided by the devices and these functionalities can be semantically described using service models [21]. The combination of the semantic and service oriented techniques can support both interoperability and scalability for the IoT.

Having semantic models and ontologies alone is not sufficient to achieve interoperability in the IoT. Ontologies developed by different parties are not guaranteed to be compatible with each other; in many cases, the research on ontology matching can be used to align the different ontologies; however, accuracy of the matching is frequently not satisfying and significant amount of human effort is still needed. Ontology reuse has been seen as an effective way to alleviate this problem; however, we suggest that bringing the Linked Data principles to the IoT is more substantial: reusing of the concepts at schema level is important, while reusing the instances or linking to the instances in existing knowledge bases is even more important. By linking to existing knowledge rather than creating repetitive one helps a Web of interlinked IoT data to facilitate navigation, discovery and more importantly, interoperability among different sources. We have seen many recent research works that make use of the Linked Data in IoT research [22] however, to realise higher level of interoperability, the IoT community needs to make data publically available and link it to the existing knowledge to create a better connected linked-data plane.

In the Future Internet there are high demands for information interoperability and Linked Data to enable automated service composition. As the

requirements for automated composition of large number of open services are defined by diverse and heterogeneous systems, it is challenging to make complex system management operations in the absence of high degree of interoperability. The Linked Data emerges as an ideal solution to resolve part of the complex information interoperability issues in the Future Internet of networks and cloud.

8.6 The Organizational Interoperability

This aspect of interoperability is also important but does not get full IoT market ttention at this moment due to other lower issues on technical and semantics. However this is a domain to follow up and it is important to note the INTEROP VLab initiative

Stemming from the Network of Excellence INTEROP-NoE (Interoperability Research for Networked Enterprise Applications and Software), INTEROP-VLab consolidates, develops and durably maintains the European research community founded by the INTEROP-NoE of integrating, joint research and dissemination activities in the domain of Enterprise Interoperability and the associated topics.

The originality of the INTEROP-VLab research programme is based on the integration of three key thematic components along the theoretical foundations, enabling technologies and exemplar applications main lines:

- Information and Communications Technology, the technological base of interoperable systems,
- Enterprise Modelling, to implement suitable organisations for interoperable systems,
- Ontology, to ensure the semantic consistency of networked organisations and solutions,

8.7 The Eternal Interoperability [28]

We are moving towards a world where everything is connected, as in particular stressed by the Future Internet and related Internet of Things vision. Yet such a goal highlights the deficiencies of today's systems platforms in achieving a fundamental property of distributed systems, namely interoperability. Faced

with the extreme heterogeneity of computational devices and networks, how can we ensure that every system can talk to every other system?

It is the above question that the CONNECT (https://www.connect-forever.eu/) project investigated, leading to the introduction of Emergent middleware that overcomes protocol mismatches on-the-fly [24]. CONNECT is an EU Future and Emerging Technologies–FET–project, which began in February 2009 and concluded end 2012. To meet its ambitious objective, CONNECT involved experts in middleware, software engineering, formal methods, machine learning, and systems dependability.

Emergent middleware facing the interoperability challenge

Interoperability is the ability for two systems to exchange, understand and use each other's data, and is a long-standing problem in the field of distributed systems. However, the emergence of pervasive computing and the Internet of Things have brought about new challenges to achieving universal interoperability. Extreme heterogeneity and spontaneous interactions are characteristics of today's complex distributed systems. Computational devices ranging from embedded devices, sensors, and smartphones through to cluster machines and the Cloud use a wide range of communication networks and middleware protocols to communicate with one another. However, as soon as two systems adhere to heterogeneous protocols (from application down to network layers) to interact with each other, interoperability is impossible. Standards are a well-established approach to rectifying these types of problems. Where two systems agree upon a standard, interoperability can be guaranteed. However, systems may encounter one another spontaneously where no such agreement is possible, and hence where the communication protocols differ they cannot interoperate.

The aim of CONNECT is to overcome interaction protocol heterogeneity at all layers, on the fly, by using a revolutionary approach that dynamically generates the necessary interoperability solution to connect two heterogeneous systems. We term this new style of middleware: *Emergent middleware.* Figure 1 illustrates an emergent middleware solution, which ensures interoperation between two networked systems by combining *message interoperability*, i.e., the ability to interpret messages from/toward networked systems and *behavioural interoperability*, i.e., the ability to mediate the interaction protocols run by the communicating networked systems, under specified non-functional properties, e.g., reliability, performance and security.

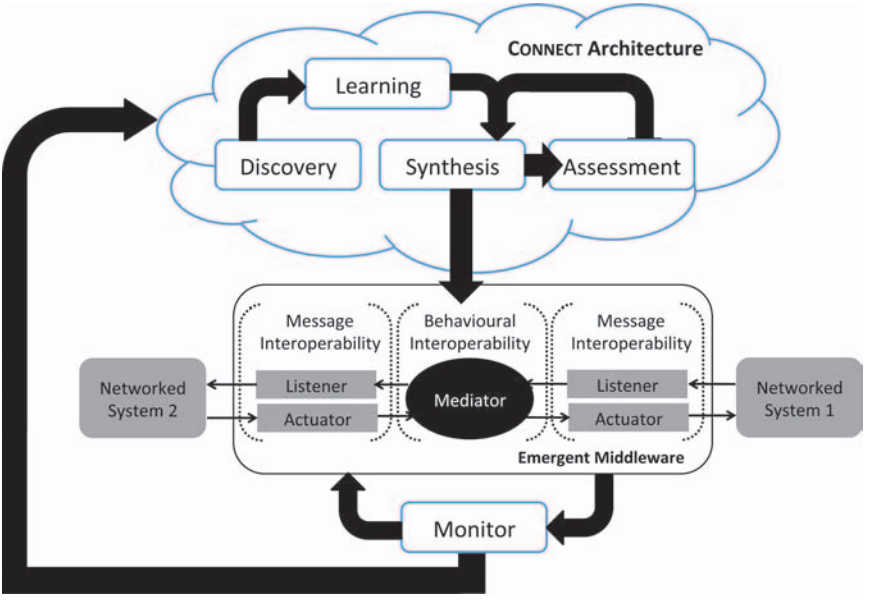

Fig. 8.9 Enabling emergent middleware.

The CONNECT *architecture* then introduces the necessary *enablers* for on-the-fly production of emergent middleware.

Network behaviourally for eternal communication

In our view, the key to eternal interoperability is to make the networking of systems agnostic to their specific technological middleware. Then, networked systems should seamlessly integrate and compose with networks of systems according to functional and non-functional properties each one of them provides to and requires from the digital environment rather than according to their underlying middleware technology.

Specifically, in the CONNECTed world, networked systems run discovery protocols to advertise their presence and locate systems with which they need to interact at a specific time and place. The initial networking association of systems is then solely based on the systems' provided and required application-specific behaviour, which is characterized semantically, thanks to ontologies. Following, CONNECT enablers present in the networked environment set up needed emergent middleware, aka CONNECTors, among the interacting systems, at run-time. CONNECTors effectively bridge semantically the protocols

of networked systems, from the application down to the middleware layer. As a result, networked technology-dependent systems interact behaviourally within the CONNECTed world, based on their respective interaction semantics. Key concepts of CONNECT are as follows:

- As pioneered by the pervasive computing domain, the *dynamic networking of digital systems* is at the heart of making networked applications evolvable and therefore eternal. In this way, a networked system is able to compose with others, based on respective provided and required functionalities within the network, without requiring a priori knowledge about the systems that are actually networked at a given time and place. Then, our only assumption is that a networked system runs some discovery protocol and further characterizes provided/required (application-layer) networked functionalities using ontologies.
- CONNECT sustains future-proof dynamic networking among any digital systems, from the legacy to the yet-to-come, by dynamically generating CONNECTors, thus bringing universal interoperability. Emergent connectors are synthesized on the fly according to the behavioural semantics of application- down to middleware-layer protocols run by the interacting parties, thereby realizing the necessary protocol mediation [25–27]. Also, emergent connectors are dependable, unobtrusive, and evolvable to indeed meet the promise of eternality, while not compromising the quality of software applications. Last but not least, emergent connectors are concrete system entities, being implemented on the fly to enable actual interactions.
- CONNECTors are implemented through a comprehensive dynamic process based on: (i) extracting knowledge from, (ii) learning about and (iii) reasoning about, the interaction behaviour of networked systems, together with (iv) synthesizing new interaction behaviours out of the ones exhibited by the systems to be made interoperable, also considering their respective provided and required non-functional specifications, finally (v) generating and deploying corresponding CONNECTors implementations to actually realize networking of the involved systems, and further (vi) continuously monitoring CONNECTors runtime behaviour, to timely detect needs of adaptation.

8.8 The Importance of Standardisation — The Beginning of Everything

Extracting from [29], Standards are driven by contributions from many individuals from a wide range of backgrounds, cultures and commercial positions. In practice, despite best efforts, there are often not enough resources to integrate these various contributions into a consistent, coherent whole.

Typical consequences of this can include:

- **Incompleteness**: often specifications are incomplete (albeit unintentionally), aspects essential to interoperability are missing or are only partially specified.
- **Inadequate interfaces** (reference points): it is not unusual for interfaces critical to interoperability to be inadequately identified or not clearly defined.
- **Poor handling of options**: A standard may contain too many options, or the options are poorly specified. For example, there may be an imprecise understanding of the consequences if certain options are not implemented. Worse still, there may be inconsistencies – even contradictions – between various options;
- **Lack of clarity:** There is a distinct skill in writing a good standard which should:
  - — be well structured;
  - — distinguish between what needs to be standardized and what does not; but should not:
  - — mix concepts;
  - — specify the same thing in several different ways;
  - — be confusing;
  - — be too verbose;
  - — be too cryptic.
- **Poor maintenance:** Lack of version control, unclear indications of exactly which requirements (mandatory and optional!) are covered by a certain release of a standard, and lax change request procedures can have a negative impact on interoperability

Incomplete, unclear standards or specifications with poorly specified options can contribute to the **biggest single cause of non-interoperability,** namely that the unfortunate implementer is forced to make potentially non-interoperable design decisions on critical parts of the system based on a lack of information.

Test for interoperability!

From [29], we can also read: The development of standardized test specifications is an integral part of the strategy for ensuring interoperability. There is no silver bullet. Testing will not eliminate all possible instances of non-interoperability, though it can do a lot to help. For example, the use of ETSI conformance test specifications in the Global Certification Forum (GCF) certification of GSM and UMTS handsets guarantees interoperability of these terminals over the air interface.

The question being asked by the ICT industry is no longer 'can we afford to test?' but rather 'can we afford not to test?'. The response is 'No! We cannot'.

In the context of standardization some SDOs such as ETSI focuses on the development of two types of test specifications, which reflect the principle: test the components first, then test the system, i.e.:

- Conformance test specifications; and
- Interoperability test specifications.

Plan for validation and testing

The approach to testing and the accompanying test specifications needs to be considered at an early stage. A well-specified standard which is validated and for which there exist high-quality test specifications is more likely to lead to interoperable products. It is important, however, that development of test specifications and activities such as interoperability events (eg Plugtests) are done in a timely manner.

8.9 The Need of Methods and Tools and Corresponding Research

From [29] on challenges related to "Designing for interoperability" we can read: Doing something well from the start does not have to be expensive.

Practice has proven that it is cheaper in the long-run, but even in the short-term there are clear benefits. Rushed, corner-cutting, muddled-headed standardization efforts with repeated returns to square one are, unfortunately, an expensive, time-wasting reality. However, these are the exceptions, rather than the rule.

There is a need for the application of pragmatic specification techniques and good working practices adapted, if necessary, for particular needs.

To avoid the kind of problems identified in previous section, advice is given on how to:

- develop clear requirements;
- develop a comprehensive architectural overview, including clear identification of interoperable interfaces;
- concentrate on specifying the right things, i.e. interoperable interfaces, and resist detailing internal implementation;
- use good protocol design techniques, such as
    - separation and description of normal behaviour and behaviour under error conditions;
    - full specification of options, including consequences of not implementing options;
    - development of (interoperability) profiles, where appropriate;
    - full specification of data (messages) and the encoding of that data;
- plan for validation and testing.

Solutions can range from the use of well-structured prose, with the correct and consistent application of the drafting rules (e.g. the use of the words shall, should, etc.), to the **judicious application of modelling techniques, tools and languages** such as:

- Unified Modelling Language (UML) for requirements specification;
- Message Sequence Charts (MSC) for the specification of information flows;

- Specification and Description Language (SDL) for detailed protocol specification;
- Abstract Syntax Notation (ASN.1) for defining message formats;
- Testing and Test Control Notation (TTCN) for writing test specifications.

Both Probe-IT [30] and IoTest [31] projects have demonstrated the useful use of TTCN in the IoT area for lower and upper layers.

TTCN-3 (www.ttcn3.org) provides an abstract language for representing many features useful for writing tests but also provide specification for test test tool architecture. Demonstrators have been developed in the Probe-IT project [30] using such methodology for lower protocols such as CoAP and 6lowpan.

IoTest project [31] demonstrates also the use of such methodology using TTCN-3 for the test of IoT services. IoTest aims to accelerate the introduction of new IoT enabled business services (in short IoT services) with effective dynamic service creation environment architecture.

IoTest in [32] describes its works on a test framework that is able to test services independently from their implementation and that requires technology independent test notations that can be executed to test and monitor prototypical applications and production systems. The UML 2.0 Testing Profile (U2TP) is a graphical notation for testing applications and systems. U2TP provides concepts for designing and developing black-box-tests [U2TP]. In accordance with UML, U2TP is only a language and therefore it only provides a notation but no guidance on how to use it. U2TP extends Unified Modelling Language Version 2 (UML 2.0) with test specific concepts like Test Architecture, Test data, Test behaviour and Test time. It reuses the UML 2.0 syntax and is based on the UML 2.0 meta-model . To realise and utilise U2TP as a test framework, the abstract U2TP notation has to be transformed into a test specific programming language like Testing and Test Control Notation Version 3 (TTCN-3) IoT.est utilizes TTCN-3 as a standardized testing notation for the inference of SUT (System Under Test) models and therefore generates technology

independent test code as a result of the knowledge based inference of a test suite.

One of the next challenges in testing is to define the test data. This process has to be carefully analysed since generating random test data may lead to redundant test cases and hence produces waste of execution and extra workload. The best idea is to intelligently generate test data so that the test data value space is covered efficiently with a small subset of values and in parallel to remove test redundancy. In this context a novel approach based on data fuzzing with TTCN-3 is being developed. Fuzz testing or fuzzing is a well-established automated and efficient black-box testing method for finding software flaws.

8.10 The Important Economic Dimension

Interoperability will not be improved without the motivation and support of market stakeholders. Motivating and involving market forces cannot be done without taking account economic dimensions. Without proper consideration of these factors, we will not succeed improving interoperability and this is often the reason why some technology stays isolated without world wide support as nobody as answer the questions of cost of testing, time to market, cost of tools, etc.

Cost of testing: Money spent on testing a product is an investment for a company. When they invest money on something, they normally expect a good return on investment. Investment on testing will impact on the market price of product. This cost includes money spent on certification programs, test house fees, purchase of test tools, etc. It also includes the money spent on correcting errors found during testing.

Time of testing has impact on the time to market and market price of a product. Time of testing is the time spent on testing a product. Using test tool to automate the test will considerably reduce the time spent on testing. We can also consider the time to develop the tests which is often under estimated.

Test tool: Cost of developing of test tool is often very expensive and can rarely be beared by one single company. There is therefore need to share

such development but for that, there is a strong needs to do so within an independent organisation, which should also itself be motivated to provide such support. Such conditions are not always met and collective actions to improve interoperability, in such case, stay in a dormant stage.

Finaly then there is a need to find a global solution which satisfy all stake holders: how to invest to the right level of test and tool, reduce my time to market and ensure the level of interoperability I need for the market and the final users.

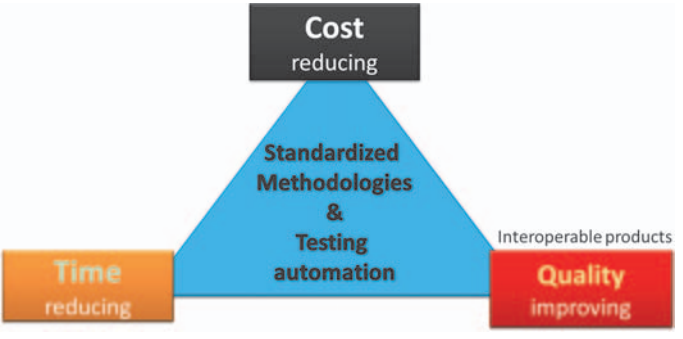

Fig. 8.10 Triple constraint triangle promoting the use of standardized methodologies.

If we use the Project Management Triangle [34] (called also Triple Constraint or the Iron Triangle) approach, we could argue that only automated, cost–effective approach with standardized methodologies and optimization/automation tools can help to find the right balance between the three dimensions. In doing so we will provide the only technical solutions to address these important economic factors.

8.11 The Research Roadmap for IoT Testing Methodologies

As for the IoT, future networks will continue to be heterogeneous, multi-vendors, multi-services and largely distributed. Consequently, the risk of non-interoperability will increase. This may lead to unavailability of some services for end-users that can have catastrophic consequences regarding applications related for instance to emergency or health, etc. Thus, it is vital to guarantee that network components will interoperate. The main way among others is to provide efficient and accurate test suites and associated interoperability testing

methodology (with associated test description/coding languages) that help in testing thoroughly both the underlying protocols used by interconnected things/machines/smart objects and the embedded services/applications.

It is really important that these new testing methods consider the real context of future communicating systems where these objects will be deployed. Indeed, contrary to most of the existing testing methods, interconnected things/machines/smart objects in the IoT are naturally distributed. As they are distributed, the usual and classical approach of a single centralized testing system dealing with all these components and the test execution is no more applicable.

The distributed nature of the tested components imposes to move towards distributed testing methods. To be more confident in the real interoperability of these components when they will be deployed in real networks, testing has to be done in a (close to) real operational environment. In this context of IoT where objects are connected through radio links, communicating environment may be unreliable and non-controllable if don't address seriously interoperability testing challenges with the same intensity and complexity of the IoT research itself. Research in IoT challenges leads to IoT validation and interoperability challenges. Previous sections have introduced the issue of improving quality while reducing costs and time to market through formalism, method and automation. For instance MBT (Method Based Testing) approach is getting growing market interest and support. To progress the use and applicability of such advanced topics to the IoT field, dedicated researches need to be undertaken and certainly not forgotten!

Researching in semantic and dynamic interoperability must have equal importance but research is already smoothly progressing due to the nature of the topics, which look more integrated into Internet research portfolio.

8.12 Conclusions

In the sequel of open issues for technical and semantic interoperability in the IoT domain a set of open issues in the form of actions to do are listed in the form of bullets and could be considered in the scope of the early requirements in the evolution of IoT. These requirements concern protocol testing and characteristics of various aspects (Linked-Data, Performance, Deployment, Scalability and Extensibility) associated with IoT applications and services.

Technical interoperability Provide confidence on IoT products to market with market-accepted level of interoperability	• Coordinate worldwide interoperability initiatives on market support specifications or protocols • Develop market acceptance roadmap • Use clear specifications development and testing methodologies leading to improve quality while reducing time and costs in a full chain optimized development cycle • Define if needed profiles to improve interoperability • Use some best practices specifications development methods • Organize interoperability events to validate specs • Use some best practices tests specifications development methods • Considered full chain specs to tool development and use methods and best practices (eg MBT) to automate and optimize development of tests and tools automatically • Develop world wide validation programmes • Pursue research in testing methodologies for IoT
Linked-Data Linking of data sources for facilitating application integration and reuse of IoT source data.	• Facilties meaning and expressions by using W3C standard Resource Description Framework (RDF) • Enable interactions between ICOs and between IoT services. • Ontology mapping/matching for re-using of semantic annotation techniques (based on Ontology Engineering) enabling descriptions of ICOs and operations. • Open linked data for building on the standards (i.e. W3C SSN standard ontology) description of sensors and ICOs. • Extension on Ontology Web Language (OWL) for extensive usage on data analytics and reasoning operations. • Enable live data analytics for processing of ICOs stream data.

Performance Focused on Mobile Application(s)/Service(s)	• ICO-related information must be handled within interactive mobile application(s). • Information updates provided either by sensor devices or external applications shall be available within the IoT middleware/application/solution in the order of minimal time of response. • There should not exist stringent latency constraints in monitoring operations for ICOs.
Deployment Dynamic establishment and reservation of services	• IoT application/service should facilitate the "Hot" deployment of sensors i.e. once an infrastructure provider deploys a new sensor, this should become available to the IoT system. • IoT application(s) should support the on-demand establishment of services, including the reservation of the required resources (for the service delivery). • IoT application(s) should support the undeployment of a service, including the release of the relevant resources.
Scalability Discovery should be enabled based on multiple criteria	• Depends on the size/scale of the IoT system(s) involved. The calculation of Key Performance Indicators (KPIs) across multiple stakeholders in the IoT system can increase the geographical and administrative scope of the application. • IoT system(s) should support the discovery of subsets of devices that can contribute to an IoT service i.e. devices that meet certain criteria pertaining to the requested service. • IoT system should be scalable and elastic in terms of the computational and storage resources that are associated with the delivery of IoT services. • The discovery could be based on a multitude of criteria including type, geographic region, sensor type, measured phenomenon, range of measurement, availability, owner or responsible party, and manufacturer and other user-defined criteria, but also combinations of all the above.

Extensibility Computational and storage resources based on Cloud infrastructures	• The system should be extensible in terms of computational and storage resources required to deliver IoT service(s). • The system should be scalable and extensible in terms of the supported ICOs. • The system should support services that leverage (potentially) thousands of ICOs distributed in tens/hundreds/thousands of different administrative domains. • The system should enable the definition / classification of new types & classes of ICOs.

References

[1] G Tselentis et al. editors, "Towards the Future Internet: A European Research Perspective", 2010, IOS Press 2009, ISBN 978-1-60750-007-0 (print), ISBN 978-1-60750-431-3 (online).

[2] J. Soldatos, M. Serrano and M. Hauswirth, "Convergence of Utility Computing with the Internet of Things", International Workshop on Extending Seamlessly to the Internet of Things (esIoT), collocated at the IMIS-2012 International Conference, 4-6 July, 2012, Palermo, Italy.

[3] NSF-funded initiative to rebuild the Internet, http://www.geni.net/

[4] Clean Slate program, Stanford University, http://cleanslate.stanford.edu

[5] Architecture Design Project for New Generation Network, http://akari-project.nict.go.jp/eng/index2.htm

[6] Michele Zorzi, Alexander Gluhak, Sebastian Lange, and Alessandro Bassi, "From today's intranet of things to a future Internet of Things: a wireless- and mobility-related view", Wireless Commun. 17, 6 (December 2010), 44–51, 2010.

[7] Michele Zorzi, Alexander Gluhak, Sebastian Lange, and Alessandro Bassi. " From today's intranet of things to a future internet of things: a wireless- and mobility-related view", Wireless Commun. 17, 6 (December 2010), 44–51, 2010.

[8] Stephan Haller, "The Things in the Internet of Things," in *Proceedings of the Internet of Things 2010 Conference*, Tokyo, Japan, 2010.

[9] Suparna De, Payam Barnaghi, Martin Bauer, Stefan Meissner, "Service modeling for the Internet of Things", 3rd Workshop on Software Services: Semantic-based Software Services, 2011.

[10] Michael Compton, Payam Barnaghi, Luis Bermudez, Raul Garcia-Castro, Oscar Corcho, Simon Cox, John Graybeal, Manfred Hauswirth, Cory Henson, Arthur Herzog, Vincent Huang, Krzysztof Janowicz, W. David Kelsey, Danh Le Phuoc, Laurent Lefort, Myriam Leggieri, Holger Neuhaus, Andriy Nikolov, Kevin Page, Alexandre Passant, Amit Sheth, Kerry Taylor. "The SSN Ontology of the W3C Semantic Sensor Network Incubator Group", Journal of Web Semantics, 2012.

[11] Cory Henson, Josh Pschorr,Amit Sheth, Krishnaprasad Thirunarayan, 'SemSOS: Semantic Sensor Observation Service', In Proceedings of the 2009 International Symposium on Collaborative Technologies and Systems (CTS 2009), Baltimore, MD, May 18–22, 2009.

[12] S. Meyer, K. Sperner, C. Magerkurth, and J. Pasquier, "Towards modeling real-world aware business processes", In Proceedings of Web of Things, 2011.

[13] M. Serrano, J. Strassner and M. ÓFoghlú, "A Formal Approach for the Inference Plane Supporting Integrated Management Tasks in the Future Internet" 1st IFIP/IEEE ManFI International Workshop, In conjunction with 11th IFIP/IEEE IM2009, 1–5 June 2009, at Long Island, NY, USA.

[14] W3C Website. http://www.w3.org/TR/PR-rdf-syntax/

[15] Horridge, M., Knublauch, H., Rector, A., Stevens, R., Wroe, C., "A Practical Guide to Building OWL Ontologies using the Protégé-OWL Plugin and CO-ODE Tools Edition 1.0" Manchester University, August. 2004.

[16] OWL Ontology Web Language. http://www.w3.org/2004/OWL

[17] FOAF. http://www.foaf-project.org

[18] SKOS. http://www.w3.org/2001/sw/wiki/SKOS

[19] W3C Semantic Sensor Network Incubator Group Report http://www.w3.org/2005/Incubator/ssn/XGR-ssn-20110628/

[20] S. De, P. Barnaghi, M. Bauer, S. Meissner, "Service modelling for the Internet of Things", in Proceedings of the Conference on Computer Science and Information Systems (FedCSIS), pp. 949–955, Sept. 2011.

[21] Wang W, De S, Toenjes R, Reetz E, Moessner K, "A Comprehensive Ontology for Knowledge Representation in the Internet of Things", International Workshop on Knowledge Acquisition and Management in the Internet of Things in conjunction with IEE IUCC, 25–27 June, 2012.

[22] P. Barnaghi, M. Presser, K. Moessner, "Publishing Linked Sensor Data", in Proceedings of the 3rd International Workshop on Semantic Sensor Networks (SSN), November 2010.

[23] W. Wang, S. De, G. Cassar, K. Moessner, "Knowledge Representation in the Internet of Things: Semantic Modelling and its Applications", special issue on Knowledge Acquisition and Management in the Internet of Things, Automatika

[24] G. Blair, A. Bennaceur, N. Georgantas, P. Grace, V. Issarny, V. Nundloll, M. Paolucci. The Role of Ontologies in Emergent Middleware: Supporting Interoperability in Complex Distributed Systems. Proc. of Middleware 2011 — 12th International Middleware Conference (2011).

[25] V. Issarny, A. Bennaceur, Y-D. Bromberg. fulltext access Middleware-layer Connector Synthesis: Beyond State of the Art in Middleware Interoperability. 11th International School on Formal Methods for the Design of Computer, Communication and Software Systems: Connectors for Eternal Networked Software Systems. LNCS 6659. Springer (Ed.) (2011).

[26] A. Bennaceur, V. Issarny, R. Spalazzese, S. Tyagi. Achieving Interoperability through Semantics-based Technologies: The Instant Messaging Case. Proc. of ISWC 2012 — 11th International Semantic Web Conference (2012).

[27] V. Issarny, A. Bennaceur. Composing Distributed Systems: Overcoming the Interoperability Challenge. Lecture Notes on HATS International School on Formal Models for Objects and Components Available. To appear (2013).

[28] Kind contribution from Valérie Issarny, Inria Paris-Rocquencourt, CONNECT coordinator
[29] H. van der Veer, A. Wiles, "Achiveing Technical Interoperability — the ETSI Approach", ETSI White Paper No.3, 3rd edition, April 2008, http://www.etsi.org/images/files/ETSI-WhitePapers/IOP%20whitepaper%20Edition%203%20final.pdf
[30] FP7 Probe-IT project www.probe-it.eu
[31] FP7 IoTest project http://ict-iotest.eu
[32] IoTest deliverable D2.1 Concepts of Goal-oriented IoT Service Composition and Testing
[33] CoAP Interoperability white paper http://www.probe-it.eu/?p=522
[34] http://en.wikipedia.org/wiki/Project_management_triangle
[35] http://www.etsi.org/plugtests/
[36] http://www.forapolis.com/website/customers/currentcustomers.aspx
[37] http://www.etsi.org/about/how-we-work/testing-and-interoperability
[38] ISO 9646: "Conformance Testing Methodology and Framework"
[39] http://www.etsi.org/technologies-clusters/technologies/testing/10-news-events/events/663-2013-6lowpan-plugtests
[40] CoAP Interoperability event March 2012- White Paper http://www.probe-it.eu/?p=522
[41] (http://mobitec.ie.cuhk.edu.hk/rfid/middleware/),
[42] (http://wiki.aspire.ow2.org/),
[43] http://www.fosstrak.org
[44] http://bullseye.xbow.com:81/Products/productdetails.aspx?sid=154
[45] http://www.mi.fu-berlin.de/inf/groups/ag-tech/projects/Z_Finished_Projects/ScatterWeb/downloads/software/ScatterViewer_UserGuide.pdf
[46] http://www.eecs.harvard.edu/~syrah/hourglass/index.shtml
[47] http://research.microsoft.com/en-us/projects/senseweb/
[48] http://sourceforge.net/projects/jwebdust/)
[49] (http://sourceforge.net/apps/trac/gsn/)

9

Semantic as an Interoperability Enabler in Internet of Things

Vicente Hernández Díaz[1], José Fernán Martínez Ortega[1], Alexandra Cuerva García[1], Jesús Rodríguez-Molina[1], Gregorio Rubio Cifuentes[1], and Antonio Jara[2]

[1]*CITSEM, Spain.*
[2]*University of Murcia, Spain.*

9.1 Introduction

Many years in the past, when mainframes where those avant-garde complicated contraptions that no anyone would dare using, not many users would think of how to interconnect them, or even if there was any need to interconnect them at all. Therefore, it did not matter whether mainframes had dramatically different features that would distinguish one from the other, nor any of their different capabilities, or how they would provide their services. However, by the end of the 1960s, there was already work in progress on how several pieces of equipment could be interconnected (for example, ARPANET), and further attempts to successfully intercommunicate computers would be tried in the next decades.

From that moment on, a new issue appeared: the electronic equipment that was used during that period of time had been very rarely conceived to interact with other elements that, despite having the same electronic nature, may behave very differently one from the other. Furthermore, if devices of different

Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, 315–342.
© 2013 *River Publishers. All rights reserved.*

ages were to be used under the same environment, how would state-of-the-art appliances coexist with legacy ones? It was not a trivial question, as computers would use different byte storage methods (little endian, big endian) and any characteristic that was not standardized — as is the case with many technologies at their first stages — was prone to differ from one device to another. It became crystal clear that when several computers were cooperating in order to perform a task, a middle layer between the hardware components, their governing operating system, and the level where applications were requested was required, as depicted in Figure 9.1, so as data being transferred from one computer from another would be intelligible by every piece of equipment implied. Thus, the middleware was conceived.

Having been coined as early as 1968 [1], "middleware" was by no means a new term at the time its general use started, but its natural abilities and the expected functionalities from this layer — abstracting all the particularities and heterogeneity of the hardware and the lower layers and providing the upper ones, mainly in charge of making service requests and responses, with homogeneous services that can be easily accessed-resulted so useful

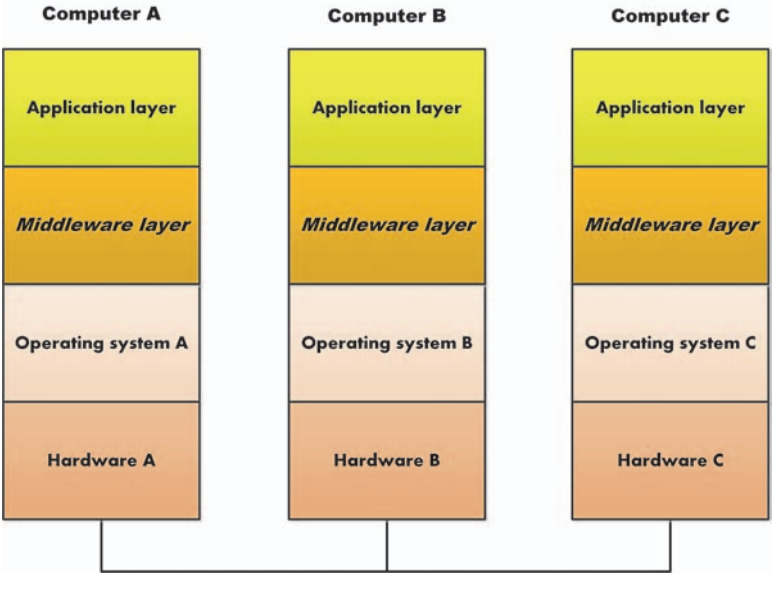

Fig. 9.1 Middleware layer between the former ones.

that actual implementations of the idea of middleware became widespread, as Remote Method Invocation (RMI), dependent on Java as the coding language, or Common Object Request Broker Architecture (CORBA). This middleware advances suited fine for the electronic capabilities and expectations of computing devices in the early 2000s, a time when computers had turned from one single huge device that would be used by several people into machines closer to a 1 computer: 1 person usage ratio.

Nevertheless, new developments on information technology were underway. It was Mark Weiser the first person to define the term ubiquitous computing back in 1988, and according to his perspective, tiny electronic devices would be incorporated to the most common entities of a regular daily routine, such as machinery, furniture or wearable pieces of garment. These tiny devices would compose a smart grid so pervasive — or, to use another word with similar connotations, ubiquitous — that the whole grid would merge with the area it was deployed onto, being used and interacted in an unconscious manner by human beings. In Mark Weiser 's own words, "Ubiquitous computing names the third wave in computing, just now beginning. First were mainframes, each shared by lots of people. Now we are in the personal computing era, person and machine staring uneasily at each other across the desktop. Next comes ubiquitous computing, or the age of calm technology, when technology recedes into the background of our lives" [2, 3]. Another definition from Mark Weiser for ubiquitous computing has been quoted by Judy York and Parag C. Pendharkar deeming ubiquitous computing as "machines that fit the human environment instead of forcing humans to enter theirs" [4]. What was also being foretold here was a shift from a computer-centric model, where one computer would be used by at least one person, to a user-centric one, with several computers surrounding a single person providing them information, services and applications. Thus, the foundations of the Internet of Things (the IoT) were established.

This new scenario does not negate the need for a middleware architecture. If something, it has become even more pressuring than before, as devices and protocols dependent and linked with the Internet of Things (mobile phones, motes, 6LowPAN, etc.) offer a plethora of new issues that have hardly ever been tackled in a combined fashion before. It has to be born in mind, though, that the middleware solutions that proved to be useful are clumsy and obsolete in the Internet of Things, mostly because they were conceived and designed at a

time that the Internet of Things was not even formulated. For example, Remote Procedure Call (RPC) has been discarded for a long time as an employable middleware solution for the Internet of Things. Among its multiple flaws, it is said about it that "RPC semantics of a synchronous, blocking invocation on a statically typed interface are overly restrictive, inflexible, and fail to provide an efficient unifying abstraction for accessing and modifying state in ubiquitous systems" [16]. Other solutions, as RMI and regular CORBA do not fare much better: Remote Method Indication switches to a more object-oriented perspective, but essentially it is a Java implementation of RPC, with the corollary of hampering any effort to make it work in a more flexible way. Additionally, RMI has the problem of providing a Java-only codification, so additional efforts in porting the code to other programming languages would be needed if other devices alien to Java are going to be used. CORBA, on the other hand, despite being an inspiration for multiple middleware architectures, will simply exceed the computing limits in most of the deployed electronic appliances in an Internet of Things-related environment [17], making it unhelpful for the purpose of services provided and, by proxy, mirroring many of the issues that have been found when trying to use the other middleware solutions.

All in all, the main challenges that must be faced by middleware when dealing with an Internet of Things-related scenario are:

- **Massive interoperability and scalability challenges.** The Internet of Things is expected to use machine-to-machine communication (M2M) at a very intense level; therefore, machines of very different characteristics — Personal Computers, laptops, embedded devices on electronic appliances, RFID tags, etc. — and capabilities will interact with each other. This will pose a serious challenge for the interoperability among these devices that will force to implement middleware layers able to interoperate an astonishing number of different devices. What is more, scalability must be offered more strongly than ever before, for the Internet of Things domain is way more dynamic in the addition of devices and their associated services. Conventional middleware solutions, with pieces of equipment that rarely change from one day to another are not fit for the almost instantaneous adoption of new elements at the network that may result in this new scenario.

- **Shrinkage of hardware and software**. Some already established devices which, in one way or another, are constrained to low power consuming or narrow bandwidth necessities, as motes in ubiquitous networking, are sure to be smaller than domestic computers, so services need to be provided at their minimum possible capabilities of transmission, energy storage, etc. This dramatic shrinking in hardware (and consequently, in software) will take its toll when creating new services and experiences, but without it ubiquitous computing would lose a part of its meaning.
- **Human intervention is reduced to its minimal expression**. As new paradigms in computing (Internet of Things, Service Oriented Computing) are developed under the ideas of Mark D. Weiser, it becomes crystal clear that if an everyday augmented element is to become part of a service provided by networked embedded systems like Wireless Sensor Networks, that supposedly is as quiet and discrete as it can be, intrusion and attention from a human being must be kept at their lowest rates (unless the end user is willing to be told about any datum related to the service) in order to have the devices participating in the Internet of Things turning into — or remain as — a silent, non-attention demanding electronic piece naturally integrated within its environment — or embedded in an object that is already like that —, which will not add extra duties or discomfort to its human beneficiaries.
- **Content and parameters under constant change**. Should OSI or TCP/IP architectures be considered as the components architecture of a service found in an Internet of Things scenario, with a physical layer at the bottom and an application layer at the top, any device is likely to find a huge number of its kind scattered through those layers: personal computers', wireless nodes' or smart phones' electronics as hardware and almost any imaginable idea as applications. Not only must an efficient middleware layer abstract the general working conditions and offer a usable interface to higher levels, but also has to deal with the changing status of applications: if a device is working in combination with, for example, a piece of clothes, services will change as the user walks or drives. In this way, some services will be lost, rendering the application built to

exploit them useless, and some other services will be discovered, activating applications already existing or downloading new ones.

Middleware should be designed properly to face this possibility and not leaving the user with only a fixed set of applications available in just a few places. Obviously, service discovery will become a major point in these architectures.

Under these circumstances, middleware architectures with functionalities beyond what is common have to be developed. Fortunately, semantics can be used to upgrade the capabilities of middleware and match the requirements that are expected from an Internet of Things deployment. In terms of information technology, semantics can be defined as *the capability of enhancing data management and how data must be processed by means of information inferring mechanisms from input data*. By using semantic middleware architectures, tasks as service discovery or device interoperability can be performed in an easier and more efficient way, for semantics will offer tools able to cope with the issues of the Internet of Things. To begin with, o*ntologies* will be provided. Although it is a term that is used in several fields, we will define ontology as *a group of terms that are typical of an area of knowledge, along with the semantic relationships among these terms*. Ontologies can be used to solve the problem of scalability, as explained in Figure 9.2: if a new device

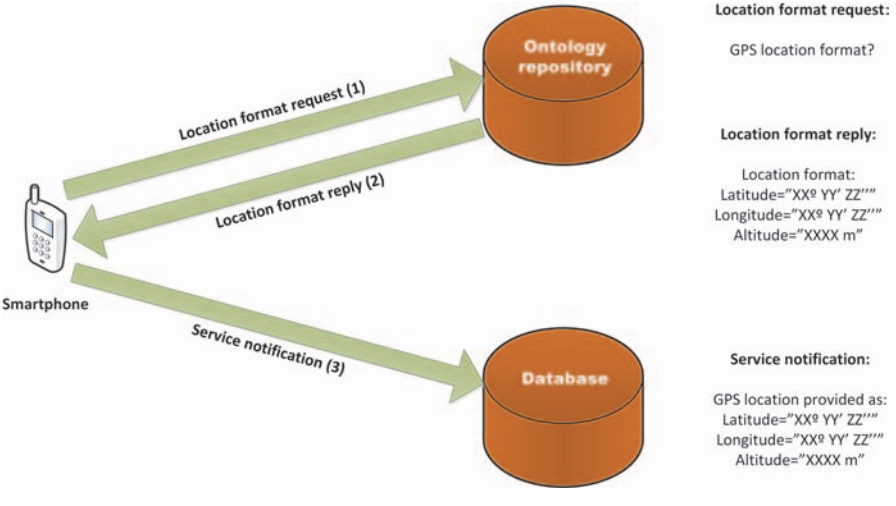

Fig. 9.2 Ontology usage example.

wants to take part of a system, it will request a repository where an ontology is stored what format needs to declare the information is able or willing to provide — shaped as services — (1). The device will get a reply dealing with the accurate format that is required (2); this format will be defined by the ontology and will be the one used in the instances of the devices using that ontology. Afterwards, the services that are provided by the device are sent to another repository — which can be the same the ontology is stored in or not — where are kept with the data of the other devices, in a sort of profile of the services that are available (3). In this way, many different devices can be added to the system at a fast pace. Interoperability is made easier as well: the data format provided by ontologies makes services equally available, regardless of the device they are being provided by.

Another significant enablers for interoperability in the Internet of Things are discovery and metadata capabilities, and therefore, key enablers for removing friction in the current IoT value chain.

One of the challenges for the IoT is to develop specifications and open source reference implementations that allow a quick market development. Thereby, IoT will be able to take off from its current status of not real business models or companies exploiting the IoT market.

The added value for the IoT can be defined with the intelligence. For this purpose, Big Data is being considered as one of the key enablers. Big Data will provide context-awareness capabilities, but for make feasible the Big Data over the IoT will require before focus on enable the IoT with semantic capabilities and context-aware discovery. The main difference between the classic data mining and the big data is the quantity of data. Therefore, IoT requires solutions founded in the Big Data principles to provide a suitable scalability for the data analysis.

Finally, an automated service discovery mechanism is required to reduce costs and automate the deployment process by removing human involvement and offline provisioning, i.e., bootstrapping phases.

For that reason, IoT requires a homogenous and suitable mechanism for the global resource discovery, devices access for the deployed smart objects in the different scenarios, sensors and devices from the end users (participative sensing), the integration of legacy and already available sensors in the smart buildings are required features for a solution based on IoT.

In this chapter, a set of protocols and technology is presented for maximizing efficiency and sustainability of IoT deployments through a resolution

infrastructure called "digcovery", this resolution infrastructure has been developed in the context of the IoT6 EU Project.

9.2 Semantics as an Interoperability Enabler

As it has been stated in the previous section, different strategies and approaches could be accomplished to diminish the interoperability challenges that the Internet of Things arises at different levels as stated in [12, 13] and [19].

The adoption of communication and hardware standards is overcoming some barriers for accessing devices resources. The devices that implement standards such as Bluetooth [5], UPnP [6], DLNA [7], Zigbee [8], 6lowPAN [9], Zeroconf [10] and so forth, could be discovered and could interchange raw data readily. Nonetheless, the way that manufacturers provide access to devices capabilities is colorful, the devices do not usually include a large set of communication interfaces for interacting with as much devices as possible, as it is not either feasible or affordable, and raw data syntax is mostly manufacturer dependent. Therefore, the interoperability challenges move to a higher level.

Service Oriented Architecture (SOA) [11] has become a worldwide adopted strategy for accessing heterogeneous systems capabilities. SOA aims at making independent two or more processes interacting over a network from the specific details of the infrastructures supporting such interaction. The SOA reference model establishes two main roles whenever two systems interact: the service client is the entity which needs a capability and the service provider is the entity with enough resources and capabilities to satisfy client needs. A service is a SOA concept that means the mechanisms that enable a client to access providers' capabilities. The SOA model also determines that a service description is also needed for assisting clients to select the most suitable service among those available, and for making public each provider offers. The syntax and the meaning of the statements in the service description must be understandable by all parts, clients and providers, based on standards. SOA implementations like Web Services [14] and RESTFul Web Services [15] really achieve SOA objectives and are worldwide accepted specifications.

The Figure 9.3, outlines how the Service Oriented Architecture paradigm could leverage interoperability of devices in the Internet of Things. Some devices like a node participating in a wireless sensors and actuators network,

could have enough resources for embed a service oriented middleware. The service oriented middleware exposes device capabilities by means of accessible services; therefore, measures from embedded sensors could be obtained by making requests to the service provider (i.e. *temperature service* and *proximity*

service components in the figure above). The middleware abstracts the service providers from the specific details of the node hardware platform, so that the same service provider could be deployed in different nodes running the same service oriented middleware.

But other devices, either legacy or resource constraint devices, would depend on the facilities provided by other powerful equipment, called gateway hereinafter, that would provide services for accessing capabilities of the real device on its behalf. The gateway will solve low level interoperability issues by complying with different communication standards, as we have already mentioned. The gateway will provide diverse communications interfaces to let as much device as possible be connected to the Internet of Things. The service oriented middleware running in the gateway would abstract service providers (i.e. *smart metering service*, *GPS service*, *biometric service* and *service for accessing sensor in legacy device*) from the heterogeneous underlying details when interacting with a device. Both the middleware deployed in the gateway and the one deployed in unconstrained devices, would also provide services for discovering new devices, choreographing new services, instantiating the service providers which would grant access to the new devices capabilities and registering those new devices, so that they become known to possible clients, either other Internet of Things devices or user applications.

Several initiatives support the above proposed idea: provide access to devices capabilities using a SOA approach. The FP7 project IoT-A, which is an IERC partner, aims at specifying an architectural reference model for the interoperability of Internet of Things systems, and has published the preliminary versions [18]. Briefly, that architectural reference model proposes, among others, that capabilities in a real device should be characterized as accessible resources, and SOA services are the way to get access to such resources.

Even though the Internet of Things systems comply with SOA, there will be still significant open issues. How do I look up the temperature sensors at home? Are *temperature sensors* and *home* understandable concepts for all the parties? Which are the mandatory services supported by any GPS device? Which are the mandatory properties of a biometric device? The use of semantics and ontologies will assist the Internet of Things architects and developers to answer to all that questions. Whenever a new device is discovered, it will be described and registered using semantic annotations complying with a specific ontology or a set of ontologies, in a manufacturer independent fashion. Therefore, the

semantic-based registry would be enabled to answer semantic requests regarding concepts in the supported ontologies: e.g. *list temperature sensors in room 4304* or *get detailed information of sensor #43*. Besides, ontologies are also envisioned for mapping devices and its mandatory services. For instance, all devices measuring temperature must at least provide access to its sampled measures by means of a specific service, and a device controlling an engine speed must at least provide a service for modifying the new desired speed.

There is a wide spectrum of ontologies describing concepts, and the relations among them, regarding main elements in an Internet of Things system: devices, services and domain-specific applications (applications for smart grids, smart cities, building management, etc.). Following, a brief description of ontologies that are becoming more influential for classifying, describing and mapping devices and services.

9.2.1 Semantic Sensor Network

Semantic Sensor Network (SSN) is an ontology for describing sensors and sensor networks developed in an OWL-DL language. The SSN ontology is able to specify the capabilities of sensors, the measurement processes and the resultant observations. It can be aligned with other ontologies which are specialized in particular contexts or domains.

SSN ontology has been developed by the W3C Semantic Sensor Network Incubator Group (SSN-XG). First, the core concepts and relations were developed (sensors, features, properties, observations, and systems). Then measuring capabilities, operating and survival restrictions, and deployments were added in turn. Finally, the alignment to DOLCE-UltraLite (DUL) and the realization of the core Stimulus-Sensor-Observation (SSO) ontology design pattern [20] were done.

The ontology can be used for a focus on any (or a combination) of a number of perspectives:

- A sensor perspective, with a focus on what senses, how it senses, and what is sensed.
- A data or observation perspective, with a focus on observations and related metadata.
- A system perspective, with a focus on systems of sensors.

- A feature and property perspective, with a focus on features, properties of them, and what can sense those properties.

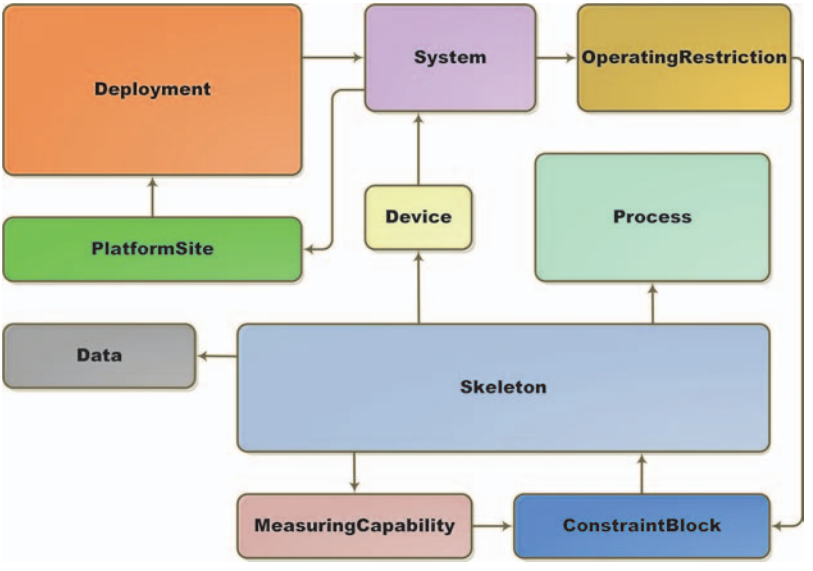

Fig. 9.4 Overview of the Semantic Sensor Network ontology classes and properties.

The full ontology consists of 41 concepts and 39 object properties, that is, 117 concepts and 142 object properties in total, including those from DUL. The SSN ontology is organized, conceptually but not physically, into ten modules, that are described in the next paragraph and pointed out in the Figure 9.4.

- ***ConstraintBlock module***: it is used to specify different ranges for conditions on a system or sensor operation.
- ***Data module***: the main task of this module is to manage data.
- ***Deployment module***: it represents the main classes and properties related to deployment of a network of sensors in the ontology.
- ***Device module***: it provides the representation of sensors, describing all its properties.
- ***MeasuringCapability module***: it offers the measurement capabilities of a sensor, for example, sensitivity, accuracy, precision, latency, etc.
- ***OperatingRestriction module***: it describes the operational and survival restrictions of the System module.

- ***PlatformSite module***: this module provides some aspects that are not covered by other modules such as spatial attributes offering different options.
- ***Process module***: this module defines the specification of the procedure implemented in a sensor.
- ***Skeleton module***: is the combination of: a number of ontology design decisions, plus re-engineering work done to align the ontology with SSO and DUL ontologies.
- ***System module***: it defines the sensing infrastructure. A system is composed by other systems called subsystems.

9.2.2 Service Ontologies

OWL-S [22] is a semantic markup for Web Services, based on OWL [21]. It is an ontology of services aiming to discover, invoke, compose and monitor Web Services readily. It is made of three main parts:

- ***the service profile***, for advertising and discovering services,
- ***the process model***, for describing service operations, and
- ***the grounding***, for providing details on how to interoperate with a service.

New ontologies based on OWL-S have been proposed, trying to meet Internet of Things systems requirements. Following is an example of one ontology proposed in the framework of the ITEA2 project DiYSE [28], an IERC partner, based on OWL-S. It adds new concepts and relations that are meaningful for services accessing resources in a device, such as security context, location, motion state, and so forth. The ontology has three parts:

- Profile: the public description of the service.
- Process: the logic of the service.
- Context: the environment in which the service is provided.

9.2.2.1 Profile

Profile is the description of the features of the service, and it must be published in an ontology repository in order to be checked by applications or other users before the use of the service. The *profile* class is composed

of *service_identification*, *service_functionality*, *security_profile* and *grounding*.

- *Service_identification* provides all the information that will let identify uniquely a service, from the set of services in an ontology repository. This identification is composed of three objects*: service_name*, the name allocated to the service, *service_explanation*, a detailed explanation of the functionality of the service, and *service_owner*, a person, entity or process name.
- *Service_funcionality* provides information about the data interchanged with the service. *Input_description* is a formal description of the input information that user (process or other) must provide to the service in a request. In the same way, *output_description* is the description of the output information generated by the service. Some services need configuration data, prior to a request that will customize the service delivery. The description of the configuration parameters is provided by the *precondition_description*.
- *Grounding* is the specification of the protocol that will support the interaction between the service and the application. The protocol could be a well-known one or could be ad-hoc for a specific application. In any case, it will be compliant with the service features.
- *Security_profile* is the description of the security framework that supports a specific service.

9.2.2.2 Context

An important element for a service oriented middleware managing information models based on ontologies is the specification of the context condition under which the service is provided. It is not the same to provide a temperature service indoor or outdoor or a heart-rate service at sea level that on top of a mountain. The context information can be stored in the ontology repository and can be used by processes to provide the service accurately.

The context class is composed of location, motion, geo_coordinates, smartSpace and context_criticality, depicted in the following figure.

Location has two subclasses, *indoor_location* and *outdor_location*. It lets know if the service is provide in an indoor location, such us a house or a public

building, or in an outdoor location such us a park, a road or a street. As it was already mentioned, the *location* can influence service delivery.

The exact positioning will be determined by *geo_coordinates*, with two subclasses, *longitude* and latitude. *Motion* will let know if the service is provided by either a static element (always in the same place) or by a mobile one. *SmartSpace* provide information about the smart space which the service belongs to. *Context_criticality* determines the importance of the context for the service delivery.

9.2.2.3 Process

Process description of the service is the most important part of the ontology, as it contains the classes related to the process that supports the service delivery.

The process class is composed of operation, atomic_process, aggregated_process, input and output.

- *Atomic_process* states that the process is atomic, so, it takes directly the information generated by sensors and provides a service. So, a simple service will be an *atomic_procees*. But, from existing simple processes in the network, it's possible to build new services, thus getting *aggregated_services* and creating "virtual sensors".
- *Aggregated_process* shows that the process is a composition of other processes and has a subclass *workflow_constructor* to indicate the way in which the processes come into play in the composed service.
- *Operation* shows the different operations that must be executed in order to provide the service. *Operation* has *input*, *output* and *precondition* subclasses. *Precondition* determines previous condition that must be met to execute the operation, if necessary, so, the operation can be customized.
- *Input*, contains the information that a process needs to start execution. *Output* contains the result of the execution of the process, once all operations have successfully ended.

In the framework of the research project ITEA2 Web of Object [23], semantic technologies are going to be applied for solve interoperability issues at the

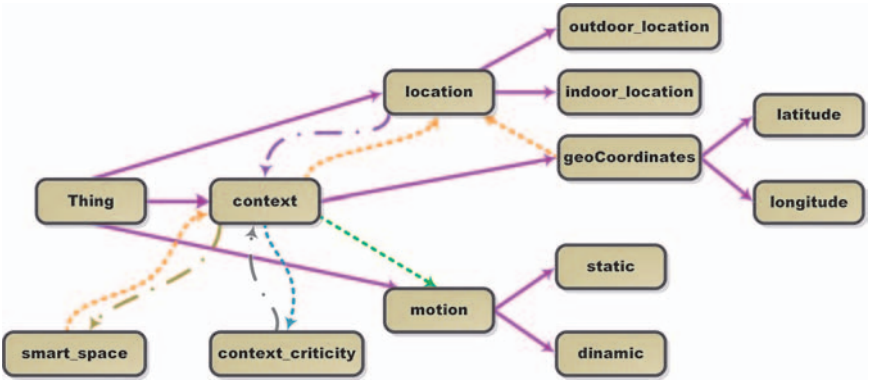

Fig. 9.5 Context condition specification.

information model layer. The services enabling access to underlying devices capabilities in a semantic service-oriented middleware (e.g. see Figure 9.3), are semantically annotated and such annotations are registered in a semantic registry. The ontology proposed merges concepts from the architectural reference model proposed in IoT-A project [18], from the previous ontology of services and from SSN.

The ontology being applied has a main class called **Entity**. It can represent a physical entity or a virtual entity. This class has two subclasses:

- **Device/Actuator**: presents the description of the device or actuator. In addition, it can represent a virtual entity.
- **Resources**: represent the resources offered by the entities.

The Figure 9.6 depicts an overview of the ontology.

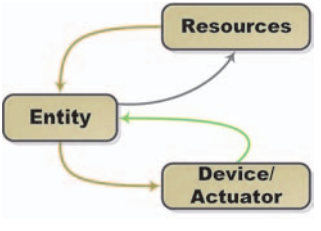

Fig. 9.6 Ontology overview.

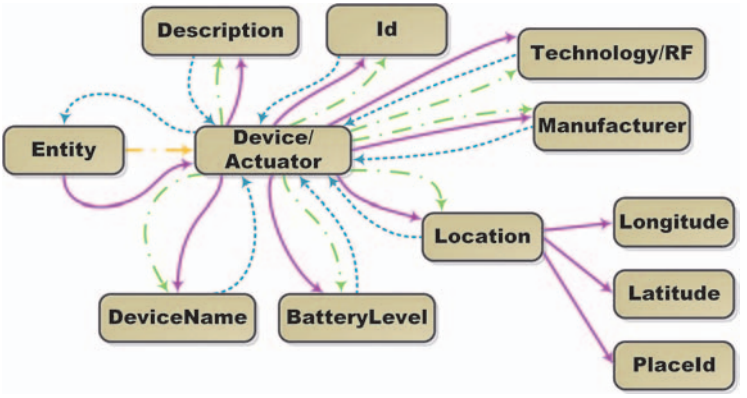

Fig. 9.7 Device/Actuator class inside the ontology.

Device/Actuator describes a device or actuator at a hardware level, describing its features. It is outlined in Figure 9.7. It must be published in an ontology repository in order to be consulted by final applications. The *Device/Actuator* class is composed by the classes:

- **DeviceName** shows the common name of this device.
- **Id** identifies the device uniquely. If the device is a virtual entity the *Id* class will be equal to the attribute "virtual" and the rest of classes would appear empty.
- **BatteryLevel** indicates the battery level of the device or actuator. Description shows a brief description about the device presenting its characteristics.
- **Manufacturer** is the manufacturer of the device.
- **Location** is a class that represents where the device is. It is composed by three subclasses: ***PlaceId*** (is a common name of the location), ***Latitude*** and ***Longitude***.
- **TechnologyRF** represents the technology used by the device in the communication, for example Bluetooth, Zigbee, Wi-Fi, etc. Finally the device can indicate its battery level using the class *BatteryLevel*.

Resources class represents the resources offered by the class *Device/Actuator*. It has one subclass called **Agent**. This class represents a piece of software which can offer one or more services. The same *Device/Actuator*

can work with one or more agents (Multi agent). It must be published in the ontology repository in order to be consulted by final applications.

The class *Agent* has two subclasses:

- **AgentName** represents the name of the agent.
- **Services** are the services given by the *Agent*. At the same time the class *Services* has three parts: ***ServiceName*** indicates the name of the service, ***Input*** is the input information that user, process or other provides to the service in order to execute the function properly, and ***Output*** which represents the output information generates by the service.

All in all, following a service registry annotation example of a temperature sensor. The annotation has been described using JSON and complies with the ontology above mentioned:

```
{
"Entity":{
     "Device/Actuator": {
        "DeviceName": "Temperature Sensor 1",
        "Id": "0014.4F01.0000.B45B",
        "Description": "Measures the environmental temperature",
        "Manufacturer": "SunSpot Oracle",
        "Location": {
           "PlaceId": "Living room",
           "Latitude": "40.6",
           "Longitude": "-3.1"
        },
        "TechnologyRF": "Zigbee",
        "BatteryLevel": "70%"
     },
     "Resources":{
        "Agent":[
           {"AgentName": "fullAgent",
           "Services": [
              {"ServiceName": "temperatureService",
              "Input": "void",
              "Output": "integer"
              },
              {"ServiceName": "batteryLevelService",
              "Input": "void",
              "Output": "integer"
              }
           ]
           },
```

```
            {"AgentName": "efficientAgent",
            "Services": [
               {"ServiceName": "temperatureService",
               "Input": "void",
               "Output": "integer"
               }
            ]
            }
         ]
      }
   }
}
```

9.2.3 Digcovery Architecture

Digcovery architecture presents as different technologies involved in the Internet of Things such as Smart Objects, RFID tags, and legacy devices are integrated into different **digrectories**. These digrectories are **managed through DNS**-queries extended with an **elastic search engine** in order to make it scalable at the same time that this offers a centralized point, called digcovery core, to manage and discover them.

All the resources and services are mapped to a common ontology and description based on existing ontologies (SSN) and profiles (IPSO), and compatible with DNS-SD types, in order to reach a **common semantic description** accessible through DNS.

This also presents how to **interoperate** with the discovery architecture through other interfaces different to DNS such as JSON and RLUS, and it will be integrated a driver to interoperate with Ubiquitous Sensor Network (USN) platform from Telefonica or Global Sensor Network (GSN) from OpenIoT.

The usage of the platform can be through DNS in order to exploit existing IP-based technologies, protocols and mechanisms, but this also presents how to carry out look-up and queries (MongoDB) over digcovery with context awareness, based on location or resource types, over the proposed MongoDB architecture, which offers organized and **context-based queries** over a heterogeneous and distributed source of resources and services.

Finally, this also offers how to manage security and privacy through access control to the services and its associated attributed and resources.

The Figure 9.8 presents the components of the digcovery architecture. The green component presents the Service Layer, whose purpose is mainly to build

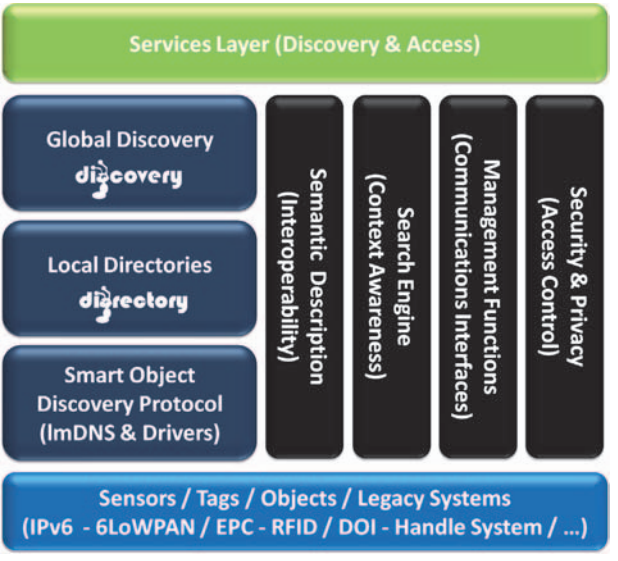

Fig. 9.8 Digcovery architecture.

the interfaces with the client applications/users through Web Services such as Restful or through Enterprise communications interfaces such as JSON/XML or specific interfaces for third party platforms such as the presented example of Global Sensor Network (GSN) platform used in the OpenIoT EU FP7 Project.

The dark blue components present the key components designed, proposed and developed in order to provide a homogenous an interoperable environment to discover, look-up and register services and resources. The main element is the digcovery, which is the global discovery platform. This platform is used to locate the different domains and the wide deployed directories with the different resources. The following elements are the directories, which contains the resources and services description from each one of the domains, these directories are not technology dependent, therefore this will be connected with any other platform through a driver. The considered platforms and the considered drivers are for the platforms such as the EPC Information System for RFID tags, and the handle system from CNIR for Digital Objects Identifiers (DOI). Finally, it has been also proposed a Smart Object Discovery Protocol based on current IPv6-based discovery protocols in order to enable the interaction between IPv6-enabled devices and the directory from its domain.

Specifically, it has been defined a lightweight version of the Domain Name Systems (DNS) extensions for local discovery based on multicast, the called mDNS, and the DNS Service Discovery semantic to describe services and resources over DNS.

The black components are the other ones key buildings blocks from the digcovery architecture. The first key component is the semantic description; it is a very important issue in order to provide a powerful IoT6 Open Service Layer. For this purpose are several the actions carried out in order EU projects such as SPITFIRE, from the European Commission with the support of events such as the Interoperability PlugFest in conjunction with Probe-IT project, and standardization groups such as IPSO Alliance, ETSI and the recent released one M2M.

The second key component is the Search Engine; this is the key element of any discovery solution in order to make it powerful. Digcovery has integrated MongoDB with some extensions based on geo-location, application profiles and domains, in order to make it feasible the context awareness look-up.

The third key component is the management functions and communication interfaces in order to interoperate with third party platforms and solutions. It has been considered CoAP to be compatible with the current Internet of Things trends, SenML and JSON to be compliance with the IPSO Alliance and IETF approaches, and other enterprise interfaces such as RLUS for management. Finally, it has been defined a port with the third party platform used in OpenIoT in order to extend and integrate the designed solution with the OpenIoT solution. The Figure 9.9 presents the communications interfaces with the different protocols.

9.3 Related Works

Currently, there are several projects that, in a way or another, make use of semantic middleware architectures, or at least that are partially inspired by them.

WoO (Web of Objects) is an ITEA2 project that, to begin with, has as its main objective creating an infrastructure for smart objects where networks and services will be deployed with independence of any proprietary protocols that may be present in the system [23, 24]. From the very beginning, WoO has been conceived to use a semantic approach in modelling devices and services,

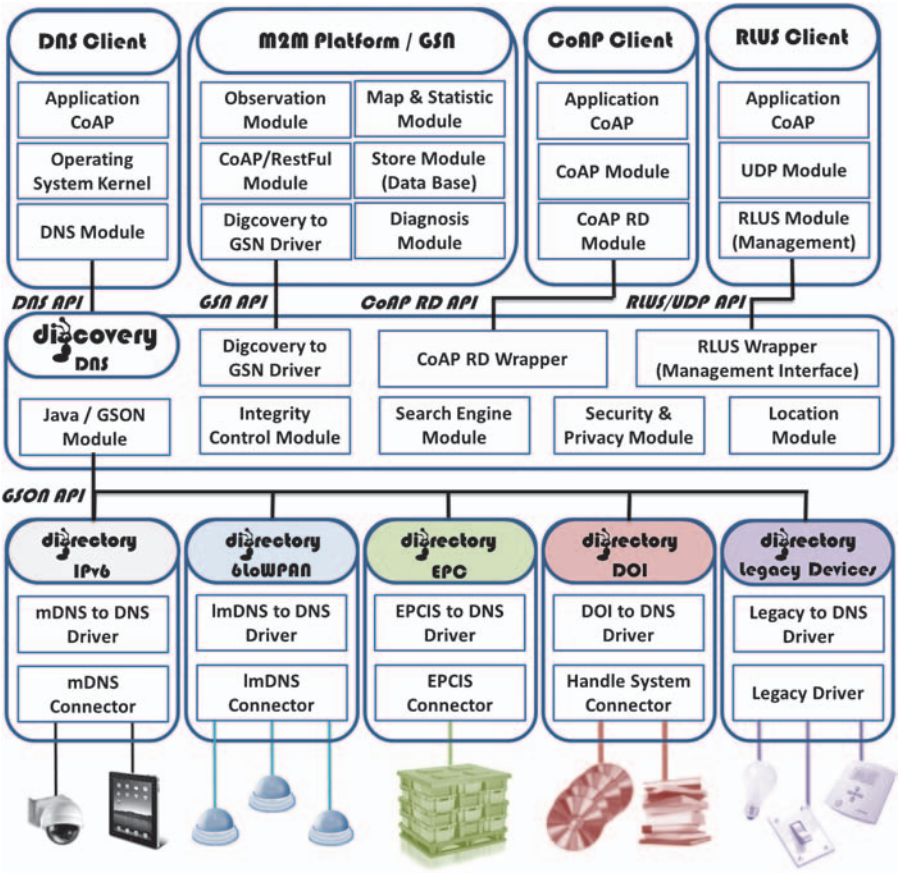

Fig. 9.9 Communication interfaces and protocols in Digcovery architecture.

along with a context-awareness approach. It is no surprise that WoO partners are interested in semantics, for interoperability is one of the key concepts of the project, along with other functionalities (service adaptation taking into account context and user profiles, dynamic reconfiguration and discovery of devices, etc.) that in an environment closely linked to the Internet of Things are best solved with semantic middleware.

Lifewear (Mobilized Lifestyle With Wearables) is another ITEA2 project [25] that aims to extend the usage of electronic devices and interfaces [26], specifically targeting physiological monitoring of real-time human body parameters (breathing rate, body temperature, heart rate) that can be

combined by environmental data (environmental temperature) to obtain different services. Stress is also put in HMI (Human-Machine Interaction) and HCI (Human-Computer Interaction) in order to further offer profiling, privacy and seamless interaction. In order to achieve these objectives, some concepts from the SOUPA ontology are used, thus providing service ontology description [27]. Interoperability is guaranteed by using a semantic middleware layer capable of integrating functionalities of low capability devices (motes, an electronically-enhanced sport belt) working with different communication protocols (Bluetooth, 802.15.4).

DiYSE (Do-it-Yourself Smart Experiences, Creating smart experiences on the Web of Things) is a project that provides the suitable tools for users to have them generating applications for the Internet of Things, even if their information technology skills are not especially high [28]. In order to do so, a semantic-based engine is used, as well as semantic descriptions for sensors, so that the latter will be better managed. Services are exposed as accessible for a group of users, and developed applications can be executed, adapted or shared. Ontologies have been used here as well — an *ad hoc* ontology is developed after OWL-S concepts —, adding the idea that they must evolve whenever either a change is required in the domain knowledge or there is a certain need of change [29, 30].

IoT-A (Internet of Things Architecture) is a FP7 project pursuing the consecution of the architectural foundations that will become dominant in the Internet of Things, in this way seamlessly integrating the disparity of the IoT architectures into a coherent architecture, which will be smart enough to federate itself with other systems already present [31]. As it happens with other projects, IoT-A relies on semantic features (Semantic Web, semantic clustering) to discover IoT resources and their dynamic association management [32]. Additionally, ontologies are used to define generic parameters as "temperature" or "luminosity", specified in terms resembling instance quantities belonging to the QU ontologies (SySML).

On the other hand, **IoT-I** (Internet of Things Initiative) is an EU Framework Programme 7 project that has as objective unifying the efforts of several communities with interests in the Internet of Things in order to work together in a similar vision of this paradigm, seeking a common strategic and technical vision for the Internet of Things and promoting a socially acceptable, economically sustainable environment that will be used to encourage the adoption

of IoT-based European technology internationally [33]. Ontologies are envisioned here as a way to improve the relations between human beings and the environment, surpassing terms as safety, security or privacy.

CASAGRAS2 (Coordination and Support Action for Global RFID-related Activities and Standardisation — 2) is another FP7 project that uses Radio Frequency Identification as a driving technology under a scope within the Internet of Things [34]. Future and existing RFID developments will be exploited as pervasive networking developments.

Ebbits (Enabling the Business-Based Internet of Things and Services) is another project looking for semantic integration of the Internet of Things into the most commonly used enterprise systems, along with interoperability between business applications [35] so as to bridge multiple stakeholders, such as services or backend enterprise applications. Ebbits provides a Service Oriented Architecture platform able to turn a subsystem or a device into a semantically-solved Web Service.

ELLIOT (Experiential Living Labs for the Internet Of Things) is a project investing efforts in developing an experimental platform strongly relying on users to create ideas, concepts and technological entities related with IoT applications and services [36].

Finally, aside from the already mentioned projects, there are many others that are involved in the development of platforms, services and applications for the Internet of Things [37]: SPRINT (Software Platform For Integration Of Engineering And Things), NEFFICS (Networked Enterprise transFormation and resource management in Future internet enabled Innovation CloudS), SmartAgriFood (Smart Food and Agribusiness), OpenIoT (Open Source Solution for the Internet of Things into the Cloud), GAMBAS (Generic Adaptive Middleware for Behavior-driven Autonomous Services), iCore (internet Connected Objects for Reconfigurable Ecosystems), IoT@Work (Internet of Things at Work), BUTLER (Secure and Context Awareness in the IoT), PROBE-IT (Pursuing ROadmaps and BEnchmarks for the Internet of Things), IoT.est (Internet of Things Environment for Service Creation and Testing), IoT6 (Universal Integration of the Internet of Things through an IPv6-based Service Oriented Architecture enabling heterogeneous components interoperability) or SPITFIRE (Semantic-Service Provisioning for the Internet of Things) [38].

9.4 Conclusions

Semantics technologies are being called to enforce interoperability in the Internet of Things systems at an information model level [19]. The shared knowledge among parties participating in such a system, provided by means of ontologies, will let them understand requests, discover new resources, look up for those needed, etc., in an unmanned way. They all know the same concepts, the relations among them and the intrinsic meaning. Therefore, non expert users could be provided with semantics tools that will assist them when creating their own applications, using resources (devices) in his environment or integrating seamlessly new ones.

There are several ongoing research project fostering the development of feasible strategies and approaches based on semantics technologies and paradigms validating the benefits of ontologies for improving interoperability in the Internet of Things systems. In the previous section, a brief list is provided, but lots are missing because the full list is quite large. All that highlights the interest of the academia and the industry sectors in such approaches.

Besides, ontologies can be merged, extended, included, etc., to promote interoperability among different ontologies. Therefore, components running in an application domain that understand an ontology could be readily integrated in a different application domain described by a different ontologies by including and redefining concepts accordingly in both ontologies. Thus, improving scalability and reusability of components in the Internet of Things systems.

Digcovery extends the existing discovery solutions through a scalable lookup based on MongoDB, JSON description of resources and the discovery of heterogeneous Internet of Things resources through the development of a REST infrastructure.

Digcovery architecture offers the denominated “digrectories” for the integration of heterogeneous resource constraint Internet of Things devices and legacy technologies.

It will be offer the framework to allow the users to register/include their own sensors into a common infrastructure, accessible/discovery the available resources through the digcovery architecture. Thereby, this will also enable the integration of opportunistic resources.

The motivation for the users to participate and include their own sensors will be the benefits of the tools and applications that collaboratively are being developed, in conjunction with the solutions that the community is defining. These tools will be mainly the data mining (Big Data) tools for data analysis, the planning tools for building dynamic logic, visualization tools for web-based and mobile platforms, the access to M2M and data storage platforms, and finally access to the data from outdoor, weather stations, prognostics, and models.

The motivation for the Telcos will be offer connectivity for the end-users sensors, i.e. offer the M2M architecture through 3G/4G networks, in addition to the Cloud-based platforms for data plan storage, as the existing USN platform from Telefonica.

The motivation for the electricity suppliers and networks is get a better prediction of the availability, planning, and offer more accurate accounting and more competitive subscription rates to the customers depending on their smart metering data.

Finally, the motivation for all is that through the collaboration and the integration of multiple data sources, it can be reached more powerful solutions, better data-analysis, more accurate data-driven modeling, situation awareness, and in definitive better solutions. For example, regarding scenarios such as smart cities and building automation be able to offer a higher energy and cost reductions for all of us.

References

[1] Naur, P., and Randell, B. (Eds.), "Software Engineering," *Report of a Conference Sponsored by the NATO Science Committee*, Garmisch, Germany, 7–11 Oct. 1968, Brussels, Scientific Affairs Division, NATO.

[2] Weiser, M., *The Computer for the 21st-Century*, Scientific American, 265, 94–104, 1995.

[3] Weiser, A., "*Hot topics-ubiquitous computing*," *Computer*, Vol. 26, No. 10, 1993, pp. 71–72.

[4] York, J., and Pendharkar, P.C., "Human–computer interaction issues for mobile computing in a variable work context," *International Journal of Human-Computer Studies*, Vol. 60, No. 5–6, 2004, pp. 771–797.

[5] Bluetooth Special Interest Group, "Home|Bluetooth Technology Special Interest Group," [Online]. Available: https://www.bluetooth.org. [Last accessed: January 2013].

[6] UPnP Forum, "UPnP Forum," [Online]. Available: http://www.upnp.org/. [Last accessed: May 2013].

[7] Digital Living Network Alliance, "Consumer Home," [Online]. Available: http://www.dlna.org. [Last accessed: April 2013].

[8] Zigbee Alliance, "Zigbee Alliance > Home," [Online]. Available: http://www.zigbee.org. [Last accessed: May 2013].

[9] 6lowPAN IETF Working Group, "IPv6 over Low power WPAN (6lowpan) — Charter," [Online]. Available: http://datatracker.ietf.org/wg/6lowpan/charter. [Last accessed: May 2013].

[10] Steinberg, D., and Cheshire, S., "Zero Configuration Networking: The Definitive Guide," O'Reilly Media, Inc., 2005.

[11] OASIS (Organization for the Advancement of Structured Information Standards), "Reference Model for Service Oriented Architecture," February 2006. [Online]. Available: http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.pdf. [Last accessed: May 2013].

[12] Khattak, A.M., Pervez, Z., Jehad Sarkar, A.M., and Lee, Y., "Service Level Semantic Interoperability," *2010 10th IEEE/IPSJ International Symposium on Applications and the Internet*, saint, pp. 387–390, 2010.

[13] Ruoklainen, T., and Kutvonen, L., "Interoperability in Service-Based Communities," *Business Process Management Workshops: BPM 2005*, C. Bussler and A. Haller, Eds., vol. 3812 of Lecture Notes in Computer Science, Springer-Verlag, pp. 317–328, Nancy, France, 2005.

[14] World Wide Web Consortium (W3C), "Web Services Architecture: W3C," 11 February 2004. [Online]. Available: http://www.w3.org/TR/ws-arch/. [Last accessed 25 January 2008].

[15] Richarddon, L., and Ruby, S., "REST ful Web Services. Web services for the real world," O'Reilly Media, Inc., 2007.

[16] Saif, U., and Greaves, D.J., "Communication primitives for ubiquitous systems or RPC considered harmful," *Distributed Computing Systems Workshop, 2001 International Conference on*, pp. 240, 245, Apr 2001. doi: 10.1109/CDCS.2001.918712. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=918712&isnumber=19870

[17] Roman, M., Mickunas, M.D., Kon, F., and Campbell, R., "LegORB and Ubiquitous CORBA," *Proceedings of the IFIP/ACM Middleware' 2000 Workshop on Reflective Middleware*. April 2000.

[18] Bauer, M., *et al.*, "Deliverable D1.4 — Converged architectural reference model for the IoT v2.0," November, 14th 2012. [Online]. Available: http://www.iot-a.eu/public/public-documents/documents-1/1/1/D1.4/at_download/file. [Last accessed May 2013].

[19] Barnaghi, P., Wang, W., Henson, C., and Taylor, K., "Semantics for the Internet of Things: Early Progress and Back to the Future," *International Journal on Semantic Web and Information Systems*, vol. 8, No. 1, 2012.

[20] World Wide Web Consortium, "W3C Semantic Sensor Network Incubator Group," [Online]. Available: http://www.w3.org/2005/Incubator/ssn. [Last accessed May 2013].

[21] World Wide Web Consortium, "OWL 2 Web Ontology Language Document Overview (Second Edition)," December 2012. [Online]. Available: http://www.w3.org/TR/owl2-overview. [Last accessed May 2013].

[22] World Wide Web Consortium, "OWL-S: Semantic Markup for Web Services," November 2004. [Online]. Available: http://www.w3.org/Submission/OWL-S. [Last accessed May 2013].

[23] Web of Objects consortium, "Web of Objects," ITEA 2 Project. [Online]. Available: http://www.web-of-objects.com/. [Last accessed May 2013].

[24] ITEA2, "Web of Objects," [Online]. Available: http://www.itea2.org/project/index/view/?project= 10097. [Last accessed May 2013].

[25] ITEA2, "Lifewear," [Online]. Available: http://www.itea2.org/project/index/view/?project=10028. [Last accessed May 2013].
[26] Lifewear consortium, "Lifewear project," [Online]. Available: http://www.lifewear.es/pages/cont/index.php?id=1. [Last accessed May 2013].
[27] Rodríguez-Molina, J., Martínez, J.-F., Castillejo, P., López, L. "Combining Wireless Sensor Networks and Semantic Middleware for an Internet of Things-Based Sportsman/Woman Monitoring Application". Sensors 2013, 13, 1787–1835.
[28] ITEA2, "DiYSE," [Online]. Available: http://www.itea2.org/diyse_project_recevies_the_prestigious_itea_silver_award_2012. [Last accessed May 2013].
[29] DiYSE consortium (Eds.), "DiYSE Report on Service Ontologies," DiYSE deliverable D3.1, page 8, 2010
[30] Flouris, G., Plexousakis, D., Antoniou, G, "A Classification of Ontology Change". In: The Poster Session of Semantic Web Applications and Perspectives (SWAP), 3rd Italian Semantic Web Workshop, PISA, Italy, 2006.
[31] IoT-A consortium, "Mission-IoT-A: Internet of Things Architecture," [Online]. Available: http://www.iot-a.eu/public/introduction/mission-collage. [Last accessed May 2013].
[32] IoT-A consortium, "D4.1-IoT-A: Internet of Things Architecture," [Online]. Available: http://www.iot-a.eu/public/public-documents/documents-1/1/1/copy2_of_d4.2/view?searchterm=semantic. [Last accessed May 2013].
[33] IoT-I consortium, "The Internet of Things Initiative — IoT-i: Internet of Things Iniciative," [Online]. Available: http://www.iot-i.eu/public. [Last accessed May 2013].
[34] CASAGRAS2, consortium, "About us | CASAGRAS2 — INTERNET OF THINGS," [Online]. Available: http://www.iot-casagras.org/about_us. [Last accessed May 2013].
[35] Ebbits consortium, "ebbits — News," [Online]. Available: http://www.ebbits-project.eu/news.php. [Last accessed May 2013].
[36] Community Research and Development Information Service, "ELLIOT. Experimental Living Lab for The Internet of Things," [Online]. Available: http://cordis.europa.eu/projects/rcn/95205_en.html. [Last accessed May 2013].
[37] IERC Cluster, "IERC-European Research Cluster on the Internet of Thins," [Online]. Available: http://www.internet-of-things-research.eu/partners. htm. [Last accessed May 2013].
[38] Spitfire consortium, "SPITFIRE. Semantic Web interaction with Real Objects," [Online]. Available: http://spitfire-project.eu/. [Last accessed May 2013].

Index

3G, 10, 19
3GPP, 67, 103, 106, 115, 139, 261, 262
6LoWPAN, 103, 117, 246, 271
6LowPAN, 287–289, 306, 317, 322

access control, 210, 213, 215, 217, 219, 226, 228, 233–237, 240, 241
accountability, 241
accuracy of the data, 222
activity chain, 211, 212, 223, 224
aggregation, 231, 237
agriculture, 32, 35
AIDC, 187, 192, 194
animal farming, 36
annotation, 282, 292, 295, 296, 310
anonymity, 233
architectural approach, 245
architecture, 245–248, 250, 251, 253
ARM, 19
authentication, 232, 234–237, 240
authorization, 210, 214–216, 220, 222
Automated Information Data Collection, 187, 194
automation technology, 164
autonomic IoT systems, 64, 68
autonomy, 230
availability, 229
awareness, 207, 221, 222, 224

BACnet, 99, 103, 105, 139
big data, 1, 32, 81, 84, 85, 117, 175, 186, 188, 191, 194, 204
biometric, 324
biotechnology, 18
Bluetooth, 96, 97, 103, 139, 322, 331, 337
business innovation, 182
business models, 247

CEN, 103
CEN/ISO, 259
CENELEC, 103, 139
CENELEC/IEC, 259
city traffic, 238
cloud, 8, 9, 14, 16, 21, 46, 50, 51, 61–63, 84, 85, 108, 117, 132, 141, 142, 260, 262, 269, 273, 283, 299, 300, 312
cloud computing, 1, 5, 8, 21, 61, 62, 85, 227, 237
CoAP, 103, 246, 287, 289, 306
cognitive, 208, 212
cognitive and autonomic systems, 208
cognitive framework, 212
cognitive management, 212
cognitive technologies, 14, 141
Communication Ecosystem, 49
communication level, 221, 222
communication protocols, 16, 45, 50, 97, 130, 141
communication standards, 262, 263, 275
communication technology, 15, 72, 75, 96, 128, 132, 141
Composite Virtual Object, 251
computation, 231, 235–237
connected energy, 183
connectivity, 230, 237
consumer, business and industrial internet, 9
contextual intelligence, 14
convergence, 3

convergence of information and communications, 14
converging science and technology, 10
correlation, 237
cyber space, 17
cyber-physical systems, 17, 19, 39, 42, 54, 55

data aggregation, 225, 237
data anonymity, 46, 50
data management, 81, 120
data manager, 200
data storage, 226, 237
DG Connect, 137
differential privacy, 233
digital society, 22
discovery, 63, 64, 66, 71, 106, 116, 127, 129, 135, 137, 282, 288, 292, 295, 296, 298, 301, 302, 311, 320, 336
distributed intelligence, 5
DLNA, 322
domotic, 36
dynamic global network infrastructure, 16
dynamic interoperability, 280, 309

eHealth, 36
electric mobility ecosystem, 45
electric vehicle, 8, 44, 47, 49, 182
embedded systems, 16, 28, 67, 115, 132
emergence, 230, 240
encryption, 233, 234, 237
energy challenge, 160, 161
energy consumption, 155, 156
energy harvesting, 66, 77, 97–101, 122, 123, 129, 140, 161, 201
energy-efficiency, 5
enforcement, 241
EPC, 173, 187, 195
ETSI, 259–261, 264, 265, 270, 275, 276
European commission, 10, 137, 140
European economy, 17
European Internet of Things Research, 1
European Research Cluster on the Internet of Things, 137
exchange of data, 225, 241
extensibility, 284, 297, 309, 312

factory of the future, 164
future internet, 1, 5, 27, 61, 69, 75–77, 94, 107, 118, 140, 142, 143, 277, 283, 285, 293–295, 298, 299
future networks, 260, 262, 273, 275

GNSS, 270
governance, 207–209, 211, 212, 220, 223, 224
GPS, 324

heterogeneity, 160, 212
heterogeneous standards environment, 263
heterogeneous wireless sensor networks, 238
hidden, 210
Horizon 2020, 5
HTTP, 103

identification, 16, 25, 36, 44, 61, 71, 95, 96, 106, 121, 127, 129–131, 136, 143, 156, 161, 187, 189, 190
IEEE, 259, 260, 270, 272, 275
IEEE 802.15.4, 96, 143, 173, 270, 271
IERC, 15, 16, 20–22, 32, 39, 92, 101, 104, 137, 141, 211, 224, 246, 259–262, 265, 273, 275
IERC definition, 16
IETF, 259, 270, 271
industrial applications, 154, 155, 158, 160, 169, 202, 204
industrial control, 9, 35
industrial environment, 154, 156, 160–162, 165, 172
industrial internet, 9, 26, 27, 32
industrial operation, 156
information challenge, 160, 161
initiatives, 259, 260
innovation, 259–261, 275
innovation cycles, 154
integrated operations, 197
integration, 278, 282, 290, 295, 299, 310
integrity, 229, 235, 240
intelligent building management systems, 52

Intelligent Transport Systems, 270, 275, 276
International Technology Roadmap for Semiconductors, 18
International Telecommunications Union, 15
Internet, 7–11, 13–15, 17–24, 26–29, 31, 32, 37, 42–44, 46, 48, 52, 53, 56, 57, 59–63, 69–78, 81, 84–86, 92, 94, 96, 97, 102, 104, 105, 107, 108, 111, 114, 116–118, 121, 122, 124, 125, 127, 131–133, 137, 139–143
Internet of Energy, 27, 28, 43, 44, 47, 141
Internet of Everything, 14, 15, 133
Internet of Media, 141
internet of People, 34
Internet of Persons, 141
Internet of Services, 141
Internet of Things, 1–8, 10, 11, 13–15, 17–24, 27, 28, 31, 32, 52, 56, 59–63, 69–78, 81, 92, 96, 97, 102, 104, 107, 108, 111, 116, 122, 124, 125, 127, 131, 132, 137, 141, 154, 162, 171, 177, 181–187, 194, 195, 197, 207–209, 211–213, 219–221, 225, 245, 246, 259, 272, 273, 275, 315, 317–320, 322, 324, 325, 327, 336–339
Internet of Things applications, 10, 19, 23, 27, 31, 56, 76, 108, 127, 131
Internet of Things architecture, 127, 132, 140, 141
Internet of Things development platforms, 58
Internet of Things Ecosystems, 3
Internet of Things European Research Cluster, 4
Internet of Things Research Needs, 131
Internet of Things strategic research and innovation agenda, 7
Internet of Things strategic research and innovation agenda, 20, 21, 72, 137
Internet of Things Timelines, 127
Internet of Vehicles, 46, 141
Internet society, 241
interoperability, 46, 52, 54, 55, 63, 67, 71, 75, 77, 90, 102–112, 118, 120, 123–125, 127, 130–132, 135, 141, 209, 220, 277–282, 285–305, 307–310, 315, 318, 320–322, 324, 330, 336–339
interoperability of objects, 5
IoT, 259–264, 266–270, 272–276
IoT applications, 14, 18, 26, 28–30, 32, 36–40, 42, 51, 54, 56, 57, 61–64, 96, 106, 113, 131, 142, 153–160, 162, 163, 170, 201–204
IoT European Research Cluster, 137
IoT industry applications, 153, 160
IoT innovation, 260
IoT platform, 227
IoT reference model, 248
IoT research, 259–262, 275
IoT standard, 259, 261, 268, 273, 275
IoT Standardisation, 259, 260, 275, 276
IP convergence, 13
IP protocol, 22, 117
IPv6, 8, 10, 18, 68, 70, 74, 75, 108, 117, 128, 133, 136, 138, 141, 246, 259, 262, 270, 271
ISA100.11a, 270
ISO, 230
ITS, 260, 270, 275, 276
ITU-T, 259, 260, 272–275

Key Enabling Technologies, 17
KNX, 99, 105, 141, 262

learning mechanisms, 256
lifetime, 156, 157, 159–161, 171, 195, 198, 200
location, 327–329, 331
location information, 266, 268
location tracking, 156
logistics, 14, 34, 53
LTE, 19, 67, 115

M2M, 8, 10, 35, 50, 61, 75, 81, 82, 103–106, 114, 130, 141, 169, 182, 187, 260–266, 273–275, 318
M2M service layer, 262–266, 273–275
MAC, 270, 271, 275
maintainability, 229
maintenance, 156, 157, 159, 169, 172–175, 198–200, 202, 204

manufacturing industry, 154, 186, 188
micro-nano devices, 210
middleware, 280, 283–285, 296, 300–302, 311, 316–320, 323, 324, 328, 330, 335–338
mobile internet, 10
Moore's Law, 18, 84
More-than-Moore, 18, 31
MOS, 18
multiple layers, 228

nanoelectronics, 16, 39
nanoelectronics, communications, 16
network technology, 75, 91, 128, 132, 137
network virtualization, 16
networked intelligent devices, 42
networking technology, 72, 75
next generation networks, 15, 67, 115
NFC, 34, 96, 129

OASIS, 259
OGC, 259, 266–270
oil and gas industry, 155, 197, 204
oneM2M, 259, 264–266
ontologies, 320, 321, 324, 325, 327, 328, 337–339
ontology, 320, 321, 324–332, 337, 339
open APIs, 3
organisations, 259, 262, 265
organizational interoperability, 279, 299

personally identifiable information, 233
pervasive systems, 208
photovoltaics, 34, 42, 101, 123, 129, 135
PHY, 270, 275
physical world, 17, 22, 32, 53, 60, 65, 69, 71, 79, 85, 86, 113, 116
platforms, 8, 9, 11, 22, 29, 30, 40, 51, 54–56, 58, 62, 82, 83, 85, 87, 91, 93, 109, 118, 120, 124, 125, 127, 133, 135, 136, 226–229, 235, 236
privacy, 207–212, 217–229, 232–234, 237, 239–241
privacy mechanisms, 233
processes, 153–156, 158, 162–168, 170, 172, 175, 176, 185, 187–193, 195, 198, 204

product life cycles, 154
protection of data, 222
public transportation, 226, 237, 238

quality assurance, 255
Quality of Information, 231

real and virtual worlds, 211
reference model, 274, 275
reliability, 158, 200, 225, 227, 229, 241
repository, 254, 256, 257, 321, 327, 328, 331, 332
research, 259–262, 265, 270, 275
Residential building ecosystem, 44
resource manager, 217
retail, 23, 32, 34
reusability, 339
revocation, 214, 217
RFID, 8, 10, 35, 84, 96, 103, 104, 129, 133, 136, 139, 143, 157, 160, 166, 171–173, 187, 194, 195, 272, 318, 338
robotics, 1, 5
robustness, 158, 204

safety, 211, 229, 237
scalability, 46, 61, 68, 74, 80, 93, 128, 133, 227, 236, 245, 251, 318, 320, 339
SDO, 262, 264, 265, 273
seamless, 218
search, 10, 35, 84, 85, 121, 129, 135, 233, 237
security, 8, 10, 12, 16, 23–26, 28, 30, 31, 34, 42, 45–47, 50, 52, 54, 55, 57, 58, 65, 68, 71, 72, 83, 92, 94, 104, 115, 116, 120–122, 129, 130, 133–136, 207–213, 218–229, 232, 234, 235, 237, 239–241
security algorithms, 222
security and privacy, 10, 16, 65, 68, 71, 72, 92, 115, 120, 129, 225, 227, 229, 239, 240
security and safety, 159
semantic, 277, 279, 281, 282, 284, 285, 291–299, 302, 309, 310, 315, 318, 320, 322, 324–327, 330, 335–339
semantic data integration, 10
semantic description, 212

semantic interoperability, 63, 109, 279, 281, 282, 291–296, 309
semantic search, 10
semantic sensor network, 325, 326
Semantic Sensor Networking, 81, 85–87
semantic technologies, 2, 63
semiconductor, 15, 18, 31, 130
sensor, 266–270, 272
sensor networks, 10, 45, 52, 81, 84–87, 90, 101, 104, 114, 128, 143
sensor Web, 266–270
sensors, 8, 12, 14, 16, 22, 24–26, 40, 41, 45, 46, 48–51, 53, 54, 56, 57, 59, 60, 65, 68, 71, 76, 79, 81–84, 86–91, 97, 99, 107, 113, 117, 119, 121, 124, 126, 129, 133, 134, 142
service level, 251, 252, 254–256
Service Oriented Architecture, 322, 338
service oriented middleware, 323, 324, 328
service-oriented architecture, 246
services, 277, 278, 282, 283, 290–299, 306, 308–312
smart buildings, 26, 32, 39, 50
smart cities, 1, 5, 25, 39, 40, 117, 133, 225–227, 260, 275
smart city, 32, 40, 41, 48, 49, 60
smart energy, 27, 32, 39, 41, 113, 114
smart environments, 8, 18, 22–24, 86
smart factory, 52, 53, 164
smart grids, 25, 27, 28, 34, 41–45, 53, 103, 113, 275
smart health, 32, 54, 56
smart home, 50, 59
smart manufacturing, 52, 54
smart metering, 34, 324
smart objects, 155, 156, 177–180, 204
smart phones, 319
smart products, 165–168
smart transport, 22, 32
smart transportation, 46, 47, 237
smart_health_platform, 55, 56
smart_home_platform, 51
SOA, 322–324
social networks, 226
software and algorithms, 128, 133
software networks, 31
software technologies, 14
SoS, 229, 230
SRA, 63, 137
Standard Development Organisations, 262
standardisation, 50, 56, 67, 96, 104, 110, 114, 115, 120, 130, 259–265, 270, 275, 276, 303
standardization, 159, 173, 204
standards, 15, 19, 42, 46, 47, 52, 67, 72, 73, 83, 96, 101–105, 109, 110, 115, 118, 123–125, 129, 130, 136, 140, 142
static interoperability, 280
storage, 210, 218, 219, 221–223
strategic business, 182
strategic research and innovation agenda, 7
strategic research and innovation agenda, 20–22, 72, 120, 137, 143
sustainability, 156, 162, 192, 204
syntactical interoperability, 279

TCP/IP, 319
TCP/IP protocol, 247
technical challenges, 160, 162
technical interoperability, 279–281, 285, 310
technology, 8, 10, 12–14, 17, 18, 20–23, 30, 32, 37, 39, 40, 42, 45, 49, 51, 54, 59, 61, 63, 69, 71, 72, 75, 81, 91, 96, 97, 99, 104, 105, 109, 125, 127–133, 135–139, 142
technology convergence, 12, 17, 30
testing, 280, 281, 286, 289, 290, 304–310
threats, 228
transparency of data usage, 222
travel plan, 238
trust, 47, 50, 58, 92, 93, 119–122, 126, 129–131, 135, 136, 225–231, 237, 240, 241

ubiquitous, 18, 65, 128, 139, 266, 272
ultra-wide bandwidth, 96
UML, 286, 305, 306
Unified Modelling Language, 305, 306
UPnP, 322

user data, 240
UWB, 35, 96, 143

validation, 103, 110–112, 123, 124, 135, 281, 285, 286, 304, 305, 309, 310
value, 153–157, 160, 162, 163, 170–173, 176, 178, 180, 183, 185–187, 190, 192, 201, 203, 204
virtual objects, 212
virtual representation, 210, 212
virtual sensors, 81, 87–91
virtual worlds, 5
visualisation, 282, 283

W3C, 86, 143, 259, 325
WAN, 262
Web services, 173, 174, 322, 327, 338
Wi-Fi, 18, 19, 26, 50
wireless devices, 210
wireless HART, 173
Wireless LAN, 173
wireless sensor networks, 10, 52, 104, 171, 176, 177
wireless sensors, 319, 322
wireless technologies, 173, 198, 199

x86, 19
XACML, 216, 217
XML, 175

zeroconf, 322
ZigBee, 35, 97, 103, 143, 173, 262, 270, 322, 331